Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
1018 WB Amsterdam

PRIMALITY TESTING USING ELLIPTIC CURVES

by Wieb Bosma

Report 85-12

Received July 1985.

PRIMALITY TESTING USING ELLIPTIC CURVES

Wieb Bosma

Abstract.

In this report some rational primality tests are described, obtained from polynomially equivalent primality tests for certain elements of $\mathbb{Z}[i]$ and $\mathbb{Z}[\rho]$ (with ρ a third root of unity). The method generalizes the well-known tests for n in $\mathbb{Z}$ depending on the partial factorization of $n-1$, replacing the group $(\mathbb{Z}/n\mathbb{Z})^*$ involved in these by the modules of points on certain elliptic curves admitting complex multiplication. Like in the rational case, congruences can be derived for possible divisors of ν in $\mathbb{Z}[i]$ or $\mathbb{Z}[\rho]$, leading to primality criteria for ν if one is able to find a sufficient partial factorization of $\nu - 1$.

Key words: primality testing, elliptic curves.

1980 Mathematics subject classification: 10A25, 14K07.

TABLE OF CONTENTS.

§0. Introduction. 2

CHAPTER I. ELLIPTIC CURVES.

§1. Elliptic curves over fields. 4

§2. The group law. 6

§3. Endomorphisms. 14

§4. Finite ground field. 20

§5. Elliptic curves over Artin rings. 30

CHAPTER II. PRIMALITY TESTS.

§6. Primality testing. 33

§7. The $\mathbb{Z}[i]$-tests. 37

§8. Pseudoprimes in $\mathbb{Z}[i]$. 41

§9. The $\mathbb{Z}[\rho]$-tests. 49

References. 53

§0. Introduction.

We present a new application of the theory of elliptic curves to primality testing.

In the first chapter the results of the "classical" theory of elliptic curves over fields, in particular finite fields, are summarized, often without proofs (our main reference for this is [TATE]); furthermore, the definition of elliptic curves is extended to allow Artin rings as ground ring, instead of only fields. In the second part we apply the results of the first chapter to primality testing, resulting in theorems containing tests for certain elements of $\mathbb{Z}[i]$ and $\mathbb{Z}[\rho]$. The tests that we develop are analogous to the well-known tests for rational primality that make use of (partial) factorizations of $n-1$, where n is the integer to be tested. In these one utilizes the group structure of $(\mathbb{Z}/n\mathbb{Z})^*$, which is cyclic of order $n-1$ only if n is prime. In our tests these $\mathbb{Z}$-modules are replaced by the $\mathbb{Z}[i]$- or the $\mathbb{Z}[\rho]$-modules of points on certain elliptic curves admitting complex multiplication by $\mathbb{Z}[i]$ (or $\mathbb{Z}[\rho]$). Generalizations to $\mathbb{Z}[i]$ and $\mathbb{Z}[\rho]$ of the methods for $\mathbb{Z}$ that make use of partial factorizations of $n-1$ to derive congruences on possible divisors of n, are first given in sections 7 and 9. Use is made here of the fact that the elliptic curves under consideration yield *cyclic* modules over the finite field arising from reduction modulo a *prime* element of $\mathbb{Z}[i]$ (resp. $\mathbb{Z}[\rho]$).

The rational primality test that makes use of the complete factorization of $n-1$ (an element of order $n-1$ in $(\mathbb{Z}/n\mathbb{Z})^*$ can be found only if n is prime) is also generalized. In doing this, by showing that we can find a point on our curves after reduction modulo ν (the element to be tested, after a proper normalization) that is annihilated by $\nu-1$ (and not by a proper divisor of it) only if ν is prime (with a few small exceptions, detected in §8), we have to make sure that these reductions are well-defined for *composite* ν too. This is taken care of in sections 2 and 5, where it is shown that elliptic curves over Artin rings can be defined in such a way that if we use the proper universal formulas for addition (and complex multiplication) of points on elliptic curves over fields, these formulas do also give the addition on curves

over Artin rings.
The resulting primality tests in $\mathbb{Z}[i]$ and $\mathbb{Z}[\rho]$ (leading to tests in $\mathbb{Z}$) are in general independent of the classical tests, and have the advantage that for testing one integer in fact a collection of independent tests is available, since different elliptic curves can be used. Moreover, it turns out that for the tests exploiting the partial factorization of $\nu - 1$, use can be made of all factors found of *associates* of ν minus 1, which means that we utilize the factored part of $\nu^4 - 1$ (in $\mathbb{Z}[i]$) or even $\nu^6 - 1$ (in $\mathbb{Z}[\rho]$).

CHAPTER I. ELLIPTIC CURVES.

§1. Elliptic curves over fields.

(1.1) Definition. An *elliptic curve* E *over a field* K is a projective non-singular algebraic curve of genus 1 with a point 0_E defined over K.

(1.2) Remarks. Recall that any projective algebraic curve C can be given by an equation $F = 0$, for some absolute irreducible homogeneous form $F \in K[X,Y,Z]$. The set of projective solutions $(x : y : z)$ to $F = 0$ in K is the set of K-rational points of C, denoted by $C(K)$. For elliptic curves, $E(K)$ is non-empty by definition. Non-singularity of C means that the three partial derivatives of F do not simultaneously vanish in any point defined over an algebraic closure $\overline{K}$ of K.
Of course there are several other definitions, equivalent to (1.1), for elliptic curves (of which we will in fact make use, see below); in terms of function fields associated to the curve E, we demand to have given a prime divisor $\underline{0}_E$ of degree 1 in a function field of one variable which is of (absolute) genus 1 (see e.g. [ROBE]).

(1.3) Weierstrass Forms. An immediate consequence of the Riemann-Roch theorem for curves is that any elliptic curve E over K can be given by a cubic equation

$$(1.4) \qquad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with coefficients $a_i \in K$ $(i=1,2,3,4,6)$.
Notice that the unique point $(0 : 1 : 0)$ at infinity $(Z = 0)$ is always K-rational; we take this for 0_E.
If the characteristic $\operatorname{char} K$ does not equal 2 or 3, we can transform the equation (1.4) into

$$(1.5) \qquad Y^2Z = X^3 + aXZ^2 + bZ^3 , \qquad a,b \in K .$$

Conversely a cubic defined by (1.4) always defines an elliptic curve provided that the discriminant Δ , defined by

$$\Delta = -(a_1^2+4a_2)^2\cdot((a_1^2+4a_2)a_6-a_1a_3a_4+a_2a_3^2-a_4^2)-8(a_1a_3+2a_4)^3-27(a_3^2+4a_6)^2+$$
$$+9(a_1^2+4a_2)\cdot(a_1a_3+2a_4)\cdot(a_3^2+4a_6) \quad ,$$

is non-zero.

In characteristic $\neq 2,3$ this means

$$\Delta = -16(4a^3+27b^2) \neq 0 \qquad \text{(with } a \text{ and } b \text{ as in (1.5))}.$$

([TATE]§2.)

(1.6) Remarks. This characterization of elliptic curves in terms of Weierstrass forms will be used to define elliptic curves over Artin rings in §5.

Since in our applications we can usually exclude the cases $\operatorname{char} K = 2,3$ we will from now on refer to the simplified equation (1.5) as the Weierstrass form of our curves (with $\Delta \neq 0$). When some results in the sequel can be obtained in these exceptional characteristics, we will sometimes just mention this without working them out in detail using (1.4).

§2. The group law.

The feature that makes elliptic curves of special interest to us, is that they form abelian varieties (of dimension 1); in particular their K-rational points constitute an abelian group. This structure is inherited from the divisor class group, which enables us to define addition of rational points via the multiplication of the corresponding prime divisors.

(2.1) Definition. Let E be an elliptic curve over a field K of characteristic $\neq 2,3$ and given in Weierstrass form (1.5).
We make the set $E(K)$ into a group by:

(2.2) taking $0_E = (0:1:0)$ as *zero element* 0 ,

(2.3) taking $-P = (x:-y:z)$ as the *opposite* of $P = (x:y:z)$ for any $P \in E(K)$,

(2.4) defining the *sum* $P_1 + P_2$ of points $P_1, P_2 \in E(K)$ via

$$P_1 + P_2 + P_3 = 0 \iff P_1, P_2, P_3 \text{ collinear} \quad ;$$

in other words: $P_3 = -(P_1 + P_2)$ is the third rational point of intersection of the straight line through P_1 and P_2 (which we take to be the tangent whenever $P_1 = P_2$) and the curve.

(2.5) Remarks. That (2.1) reflects multiplication of divisor classes is of course a proposition rather than a definition (see e.g. [HART]Ch.IV, [ROBE]Ch.II). For a proof of the fact that this definition furnishes $E(K)$ with an abelian group structure without reference to divisor classes see [FULT]Ch.5 .
Definition (2.1) has the following well-known real-geometric interpretation (see figure 1):
by (2.2) and (2.3) the zero element 0_E can be thought of as lying infinitely far off in the direction of the y-axis (lying on every vertical line), and according to (2.4) the sum $P_1 + P_2$ can be found by reflecting

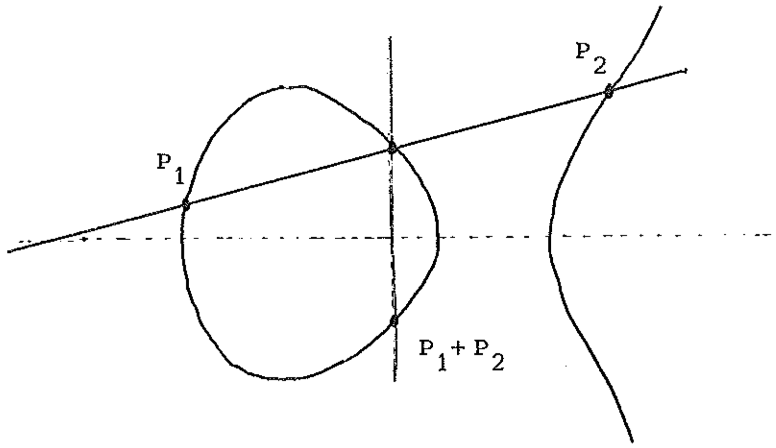

Figure 1.

the third intersection point of the line through P_1 and P_2 (tangent if $P_1 = P_2$) in the x-axis.

(2.6) Formulas. The addition of points as defined in (2.1) can be made quite explicit in terms of the coordinates. Classically this is done distinguishing three different cases:

(i) either P_1 or P_2 equals 0_E , or $P_1 = -P_2$;

(ii) case (i) does not apply and $P_1 \neq P_2$;

(iii) case (i) does not apply and $P_1 = P_2$.

Case (i) is the simplest, the sum $P_1 + P_2$ then being P_1 , P_2 or 0_E respectively. In the second case, one finds an equation for the line determined by P_1 and P_2 :

$$L : Y = \lambda X + \nu \qquad \text{(we can work affinely now)}$$

with $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ and $\nu = \dfrac{x_2 y_1 - x_1 y_2}{x_2 - x_1}$

writing $P_i = (x_i, y_i)$ for $i=1,2$.

Subsequently, the coordinates of the third point of intersection of L with E give $P_3 = -(P_1 + P_2)$.

In the third case one proceeds similarly, but now L is replaced by the tangent at P_1 , so λ is found as quotient of the partial derivatives of the affine equation for E .

(2.7) Comments. For our purposes the resulting formulas are not satisfactory; to be able to define addition in the next sections on curves over certain rings, we would like to have formulas for addition on *open* subsets of the curve. Since addition is a map $E(K) \times E(K) \to E(K)$ we would like to have a finite open covering of $E(K) \times E(K)$ (defined by typically "open conditions" $G \neq 0$ for some polynomial G in the coordinates of the points and the Weierstrass coefficients of the curve), such that an arbitrary pair $(P_1,P_2) \in E(K) \times E(K)$ is contained in an open on which addition is given uniformly, for every E and K, by polynomials in the coordinates of (P_1,P_2) and the coefficients of the Weierstrass form.

Fortunately we can always achieve this. We formulate this property as follows.

(2.8) Assertion. There exist $k \in \mathbb{Z}_{>0}$ and for every $i \in \mathbb{Z}$ with $1 \leq i \leq k$, elements Q_i, R_i, S_i and $T_i \neq 0$ of $\mathbb{Z}[A,B,\frac{1}{D},\frac{1}{6}][X_1,Y_1,Z_1,X_2,Y_2,Z_2]/(F_1,F_2)$ (in which $D = -16(4A^3+27B^2)$ and $F_j = Y_j^2Z_j - X_j^3 - AX_jZ_j^2 - BZ_j^3$ for $j = 1,2$) with T_i homogeneous, and Q_i, R_i, S_i bihomogeneous of the same bidegree, such that:

for every field K with $\operatorname{char} K \neq 2,3$, and

for every elliptic curve $E : Y^2Z = X^3 + aXZ^2 + bZ^3$, with $a,b \in K$ and with $\Delta = -16(4a^3 + 27b^2) \neq 0$,

we have for every pair of points $P_1 = (x_1 : y_1 : z_1) \in E(K)$ and $P_2 = (x_2 : y_2 : z_2) \in E(K)$ that

(2.9) for at least one i $(1 \leq i \leq k)$: $T_i(a,b,\frac{1}{\Delta},x_1,y_1,z_1,x_2,y_2,z_2) \neq 0$

and

(2.10) for every i $(1 \leq i \leq k)$ with : $T_i(a,b,\frac{1}{\Delta},x_1,y_1,z_1,x_2,y_2,z_2) \neq 0$

one has $P_1 + P_2 = (Q_i(a,\ldots,z_2) : R_i(a,\ldots,z_2) : S_i(a,\ldots,z_2))$.

(2.11) Remark. Again of course essentially the same applies in characteristics 2 and 3, with A and B (resp. a and b) replaced by A_1, A_2, A_3, A_4, A_6 (resp. $a_1, \ldots, a_6$) and with the appropriate Weierstrass forms etc. .

(2.12) Remark. It turns out (see below) that we can add on E as in (2.8) using only three triples of formulas (Q_i, R_i, S_i), so essentially we can take $k = 3$ in (2.8); see also [LA-RU] . This may be the minimal value for k, but a proof for this is lacking.

(2.13) Proof of (2.8). We give a constructive proof, distinguishing three cases. Let E and K be given as above.

The first case is in fact the "generic" classical case (2.6)(ii):

(2.14) $\quad P_1 \neq P_2$ and $P_1 \neq 0_E \neq P_2$.

We intersect $L : Y = \lambda X + \nu Z$

where $\lambda = \dfrac{y_2z_1 - y_1z_2}{x_2z_1 - x_1z_2}$ and $\nu = \dfrac{x_2y_1 - x_1y_2}{x_2z_1 - x_1z_2}$

and $E : Y^2Z = X^3 + aXZ^2 + bZ^3$.

This leads to an equation of degree 3 in $\frac{X}{Z}$, of which we know the roots $\frac{x_1}{z_1}$ and $\frac{x_2}{z_2}$; thus we find

$$\frac{x_3}{z_3} = \lambda^2 - \left(\frac{x_1}{z_1} + \frac{x_2}{z_2}\right) .$$

Writing this and the resulting formula for $\frac{y_3}{z_3}$ out, we find after reduction modulo the Weierstrass equation and after removing common factors z_1z_2, formulas Q_1, R_1, S_1.

It turns out that these do also apply in case either $P_1 = 0_E$ or $P_2 = 0_E$ (but not both), which implies that they are valid on the union of the opens defined by $T_{11} \neq 0$, $T_{12} \neq 0$:

(2.15) $\quad T_{11} = X_1Z_2 - X_2Z_1 \qquad T_{12} = Y_1Z_2 - Y_2Z_1$.

The second set of formulas gives addition near the diagonal of $E(K) \times E(K)$. For, if

(2.16) $P_1 = (x_1 : y_1 : z_1)$ and $P_2 = (x_2 : -y_1 : z_1)$ with $x_2 \neq x_1$

then using the equation for E we may write

$$\frac{y_2z_1-y_1z_2}{x_2z_1-x_1z_2} = \frac{x_1^2z_2^2 + x_1x_2z_1z_2 + x_2^2z_1^2 + az_1^2z_2^2}{(y_1z_2 + y_2z_1)z_1z_2} .$$

Taking this for λ in the equation of L above, we get formulas Q_2, R_2, S_2 . The open set where they are valid is characterized by $T_{21} \neq 0$ or $T_{22} \neq 0$:

(2.17) $T_{21} = Y_1Z_2 + Y_2Z_1$ $\qquad T_{22} = X_1^2Z_2^2 + X_1X_2Z_1Z_2 + X_2^2Z_1^2 + AZ_1^2Z_2^2$.

Finally, since the only pair (P_1,P_2) not covered yet is $(0_E,0_E)$, we derive formulas for a neighbourhood of $(0_E,0_E)$.

Here we use $y_1y_2 \neq 0$, and using the equation for E again, we get

(2.18) $$\frac{y_2z_1 - y_1z_2}{x_1y_2 - x_2y_1} = \frac{x_1^2y_2^2 + x_1x_2y_1y_2 + x_2^2y_1^2 + ay_1y_2z_1z_2}{y_1^2y_2^2 - ax_1y_2^2z_1 - ax_2y_1^2z_2 - by_2^2z_1^2 - by_1y_2z_1z_2 - by_1^2z_2^2}$$

Taking this for μ in the equation for the line, that now reads

$$L' : \quad Z = \mu X + \omega Y$$

gives after intersection with E formulas Q_3 , R_3 , S_3 which are valid at least on the open given by

(2.19) $T_3 \neq 0$

where T_3 is, if we do not make any effort to simplify it, a polynomial that is bihomogeneous of bidegree (9,9) .

That completes the proof of (2.8). □

<u>(2.20) Remarks</u>. Notice that (for $j = 1,2$) F_j is Eisenstein at Z_j as a polynomial in X_j and therefore (F_1,F_2) is a prime ideal: $\mathbb{Z}[A,B,\frac{1}{D},\frac{1}{6}][X_1,Y_1,Z_1,X_2,Y_2,Z_2]/(F_1,F_2)$ is a domain.

Furthermore the T_i together generate this whole ring as an ideal: $(T_1,\ldots,T_k) = (1)$, for else they would all be contained in some maximal ideal in whose residue class field (which is of characteristic $\neq 2,3$ and in which F again determines an elliptic curve since both 6 and D are invertible in the ring) they would thus all vanish simultaneously in contradiction to (2.8).

We will now mention some important corollaries for the universal formulas of (2.8), which we will prove below all at once after a short explanation. We use the notations of (2.8).

(2.21) Corollary.

For every $i \leq k$: $\quad R_i^2 S_i - Q_i^3 - AQ_i S_i^2 - B_i S_i^3 = 0.$

(2.22) Corollary.

For every $i,j \leq k$: $Q_i R_j - Q_j R_i = 0$, $R_i S_j - R_j S_i = 0$, $Q_i S_j - Q_j S_i = 0$.

(2.23) Corollary. Let for $U \in \{Q, R, S\}$ the elements $\overline{U}_i$ (for $i \leq k$) of $\mathbb{Z}[A,B,\frac{1}{D},\frac{1}{6}][X_1,Y_1,Z_1,X_2,Y_2,Z_2]/(F_1,F_2)$ be given by:

$$\overline{U}_i(X_1,Y_1,Z_1,X_2,Y_2,Z_2) = U_i(X_2,Y_2,Z_2,X_1,Y_1,Z_1) ,$$

then $\quad Q_i\overline{R}_i - \overline{Q}_i R_i = 0$, $R_i\overline{S}_i - \overline{R}_i S_i = 0$, $Q_i\overline{S}_i - \overline{Q}_i S_i = 0$.

(2.24) Corollary. Let for $U \in \{Q, R, S\}$ the elements U_{ij} , U'_{ij} of $\mathbb{Z}[A,B,\frac{1}{D},\frac{1}{6}][X_1,Y_1,Z_1,X_2,Y_2,Z_2,X_3,Y_3,Z_3]/(F_1,F_2,F_3)$ be given by $(i,j \leq k)$

$$U_{ij} = U_i(Q_j(X_1,Y_1,Z_1,X_2,Y_2,Z_2),R_j(X_1,Y_1,Z_1,X_2,Y_2,Z_2),S_j(X_1,Y_1,Z_1,X_2,Y_2,Z_2), X_3,Y_3,Z_3) \quad \text{and}$$

$$U'_{ij} = U_i(X_1,Y_1,Z_1,Q_j(X_2,Y_2,Z_2,X_3,Y_3,Z_3),R_j(X_2,Y_2,Z_2,X_3,Y_3,Z_3), S_j(X_2,Y_2,Z_2,X_3,Y_3,Z_3)) ,$$

then for every $i,j,m,n \leq k$ all of

$$Q_{ij}R'_{mn} - Q'_{mn}R_{ij} \ , \ R_{ij}S'_{mn} - R'_{mn}S_{ij} \ , \ Q_{ij}S'_{mn} - Q'_{mn}S_{ij}$$

are equal to zero in the above ring (in which F_3 has obvious meaning).

(2.25) Remark. Informally we may explain these as follows.

Corollary (2.21) merely states that for every i the set of formulas

Q_i , R_i , S_i yield a point satisfying the Weierstrass equation, provided that they do not all vanish (which may happen when $T_i \neq 0$); thus it expresses that the map $E(K) \times E(K) \to E(K)$ is well-defined.
According to (2.22), whenever $(Q_i : R_i : S_i) \neq (0:0:0) \neq (Q_j : R_j : S_j)$ both projective points are the same: on the open defined by $T_i \neq 0 \neq T_j$ the sum of two points defined either way is the same.
Corollary (2.23) formally states commutativity of the mappings defined by Q_i, R_i, S_i : when $P_1 + P_2$ and $P_2 + P_1$ computed this way yield both good projective points, they coincide (but we do not rule out that on some closed set only one of them gives $(0:0:0)$).
Finally, (2.24) expresses the associativity of addition on E : whenever both $\Psi_i(\Psi_j(P_1,P_2),P_3)$ and $\Psi_i(P_1,\Psi_j(P_2,P_3))$ are good projective points, they coincide (where Ψ_i denotes addition using the formulas Q_i etc.).

(2.26) Proofs. Let K_0 be the field of fractions

$$Q(\mathbb{Z}[A,B,\tfrac{1}{D},\tfrac{1}{6}][X_1,Y_1,Z_1,X_2,Y_2,Z_2]/(F_1,F_2)) \;;$$

then $Y^2Z = X^3 + AXZ^2 + BZ^3$ defines an elliptic curve over K_0 and this equation is satisfied by the images of the coordinates of $P_1 = (X_1 : Y_1 : Z_1)$ and $P_2 = (X_2 : Y_2 : Z_2)$ in K_0 . Moreover the images of the T_i are non-zero elements of K_0 , and therefore according to (2.8) addition on all of $E(K_0)$ is given by each of the triples Q_i, R_i, S_i . This immediately implies (2.21) and (2.22). Then (2.23) also follows. For the proof of (2.24) we observe that it suffices to prove

(2.27) if $G(Q_i,R_i,S_i) = 0$ for some $G \in \mathbb{Z}[A,B,\frac{1}{D},\frac{1}{6}][X,Y,Z]$
then $G \in (F)$

in which F denotes the Weierstrass form as usual; for in that case the isomorphism $\mathbb{Z}[A,B,\frac{1}{D},\frac{1}{6}][X,Y,Z]/(F) \simeq \mathbb{Z}[A,B,\frac{1}{D},\frac{1}{6}][Q_i,R_i,S_i]$ as subrings of $\mathbb{Z}[A,\ldots,X_1\ldots,Z_2]/(F_1,F_2)$ yields an isomorphism between the subrings $\mathbb{Z}[A,B,\frac{1}{D},\frac{1}{6}][X_1,Y_1,Z_1,X_2,Y_2,Z_2]/(F_1,F_2) \simeq \mathbb{Z}[A,B,\frac{1}{D},\frac{1}{6}][Q_i,R_i,S_i,X_3,Y_3,Z_3]$

of the ring in three variables, and so on, whence by a reasoning similar to the above, but now in the field of fractions of $\mathbb{Z}[A,B,\frac{1}{D},\frac{1}{6}][X_1,Y_1,Z_1,X_2,Y_2,Z_2,X_3,Y_3,Z_3]/(F_1,F_2,F_3)$, the result follows. Which leaves (2.27) to prove.

Let therefore first $H \in \mathbb{Z}[A,B,\frac{1}{D},\frac{1}{6}][X,Y,Z]/(F)$ be a *homogeneous* polynomial with $H(Q_i,R_i,S_i) = 0$; then by (2.22) for all $j \le k$: $H(Q_j,R_j,S_j) = 0$. Since for every field K and every point $P \in E(K)$ the sum $P + 0_E = P$ is given by some triple $(Q_j(P,0_E) : R_j(P,0_E) : S_j(P,0_E))$ we find that $H(P) = 0$ for every point over every field, so $F|H$.

Let G be arbitrary in the ring with the property that $G(Q_i,R_i,S_i) = 0$. We next use that the Q, R, S are bihomogeneous of the same bidegree (m,n) , fixing and omitting all subscripts i . First notice that always $(m,n) \neq (0,0)$ since otherwise $(Q : R : S) = (c : d : e)$ for constants $c,d,e \in \mathbb{Z}[A,B,\frac{1}{D},\frac{1}{6}]$ implying that Q, R, S satisfies e.g. the homogeneous equation $cY - dX = 0$. Since $cY - dX$ is clearly not contained in (F) , we get a contradiction to the above. So suppose $m > 0$; then $Q(\lambda P_1,P_2) = \lambda^m Q(P_1,P_2)$ and so on, but now writing $G = \Sigma H_d$ as sum of its homogeneous parts H_d of degree d , we find that $0 = G(Q,R,S) = \Sigma H_d(Q,R,S)\lambda^{md}$ as polynomial in λ , which by the above implies that each of the H_d , and therefore G itself, is contained in the ideal (F) .

This ends the proofs of the corollaries. □

(2.27) Remark. Notice that these corollaries imply that from the outcome of the computation we can judge whether we were allowed to use the formulas Q_i, R_i, S_i or not: the result is either a good projective point which can only be the desired sum (by (2.21) and (2.22)), or it is $(0 : 0 : 0)$, which can easily be recognized.

§3. Endomorphisms.

In the previous sections we defined elliptic curves over fields; we now want to study morphisms $\phi : E_1 \to E_2$ between them, in particular in case $E_1 = E_2$.

(3.1) Definitions. A *homomorphism* between two elliptic curves E_1 and E_2 , both defined over a field K , is a rational map $\phi : E_1 \to E_2$ between the curves (as varieties) which is also a group homomorphism (which just means that we require $\phi(0_{E_1}) = 0_{E_2}$). An *isogeny* is a surjective homomorphism of elliptic curves; in fact a homomorphism is surjective as soon as it is non-zero. Any isogeny corresponds to an injective field homomorphism $F_2 \to F_1$ of the corresponding function fields. The *degree* of an isogeny is the degree of this field extension $\deg \phi = [F_1 : \mathrm{im}\, F_2]$. For the zero map we define $\deg 0 = 0$. Every *isomorphism* (homomorphism having two-sided inverse) is then an isogeny of degree 1 .
An *endomorphism* of an elliptic curve is a homomorphism $\phi : E \to E$ from E to itself, i.e. either an isogeny or the zero map (denoted by 0_E).
The set of endomorphisms of E over K is made into a ring, and denoted by $\mathrm{End}_K(E)$, under
addition: $(\phi + \psi)(P) = \phi(P) + \psi(P)$ and
composition: $(\phi \circ \psi)(P) = \phi(\psi(P))$ for all $P \in E(K)$.
The units of $\mathrm{End}_K(E)$ are the *automorphisms* $\mathrm{Aut}_K(E)$.
An isogeny is called *separable* whenever the corresponding function field extension is separable; in that case $\deg \phi = \# \ker \phi$.
Every homomorphism $\phi : E_1 \to E_2$ over K gives rise to a mapping between the tangent spaces, the differential mapping $d\phi : \theta_{E_1} \to \theta_{E_2}$; this induces an adjoint K-homomorphism $\phi^* : \Omega^1_{F_2} \to \Omega^1_{F_1}$ on the K-vector spaces of one-dimensional regular differential forms. But for elliptic

curves over K, the space Ω_F^1 is just of dimension one over K, so $\mathrm{Hom}_K(\Omega_{F_2}^1,\Omega_{F_1}^1)$ is isomorphic to K itself. If we take $E_1 = E_2 = E$, it can be shown that the map $\phi \to \phi^*$ is an anti-ringhomomorphism:

$$(3.2) \qquad \mathrm{End}_K(E) \to \mathrm{Hom}_K(\Omega_F^1,\Omega_F^1) \simeq K .$$

The kernel of this homomorphism, the endomorphisms with differential zero, are just the inseparable isogenies and the zero map 0_E. Finally we note here that for elliptic curves the *invariant* differential one-forms (which are by definition those that are invariant under the translations on the curve, given by addition of a fixed point) are just the regular differential forms, and therefore generated over K by e.g.

$$(3.3) \qquad \omega = \frac{dx}{y} \; ,$$ an invariant differential on E in Weierstrass form (1.5). (For all this see [TATE],[SH-TA]CH.I,[SHAF]Ch.III .)

(3.4) Examples. Apart from the trivial endomorphisms $1_E = id_E$ and 0_E on every E there is an endomorphism defined by inverting points,

$$-1_E : P \to -P \qquad \text{for all } P \in E(K) ,$$

which is for E in Weierstrass form (1.5) given by

$$-1_E : (x:y:z) \to (x:-y:z) .$$

Also for every $n \in \mathbb{Z}_{\geq 0}$ there is an endomorphism given by multiplication with n, $n_E : P \to nP = P + \ldots + P$ (n times), for all $P \in E(K)$. One can show that these multiplications - now defined for every integer - have degree $\deg n_E = n^2$, and that they are separable if and only if $(\mathrm{char}\, K, n) = 1$.

(3.5) Corollary. For every E there is an injection $\mathbb{Z} \to \mathrm{End}_K(E)$. □

The two examples now following will be of major interest to us in the next chapter and will therefore serve as illustration throughout the rest of this chapter.

(3.6) Example. Let the curve E be given (over $\mathbb{C}$ say) by

$$E: \; Y^2Z = X^3 - AXZ^2 \qquad \text{for some } A \in \mathbb{C}^* .$$

This curve admits multiplication by i, an endomorphism defined by

$$i_E : (x:y:z) \to (-x:iy:z) \qquad \text{for every point on } E .$$

This is an automorphism satisfying $i_E^2 = -1_E$.

We thus have in this case $\mathbb{Z}[i] \hookrightarrow \mathrm{End}_{\mathbb{C}}(E)$, and we say that E has *complex multiplication by* $\mathbb{Z}[i]$.

(3.7) Example. Similarly the elliptic curve

$$E: \; Y^2Z = X^3 + BZ^3 \qquad \text{for some } B \in \mathbb{C}^* ,$$

admits *complex multiplication by* $\mathbb{Z}[\rho]$, where the primitive third root of unity ρ acts by

$$\rho : (x:y:z) \to (\rho x:y:z) \qquad \text{for every point on } E .$$

(3.8) Example. There is another important example for curves over finite fields, the so-called *Frobenius*-endomorphism Frob. It acts on E, defined over the finite field $\mathbb{F}_q$ of $q = p^k$ (p prime) elements, by raising coordinates in the q^{th} power:

$$\mathrm{Frob} : (x:y:z) \to (x^q : y^q : z^q) \qquad \text{for every point on } E .$$

For every intermediate field $\mathbb{F}_q \subset \mathbb{F}_{q^m} \subset \overline{\mathbb{F}}_q$ it is a purely inseparable element of $\mathrm{End}_{\mathbb{F}_{q^m}}(E)$ with $\deg(\mathrm{Frob}) = q$. In fact it is clear that $E(\mathbb{F}_{q^m})$ corresponds precisely to the points of $E(\overline{\mathbb{F}}_q)$ satisfying $\mathrm{Frob}^m(P) = P$.

From the fact that an elliptic curve is its own Jacobian it can be deduced that (cf. [TATE], [CASS]) associated to any isogeny $\phi : E_1 \to E_2$ there is a dual isogeny $\hat{\phi} : E_2 \to E_1$ with the property that $\phi \circ \hat{\phi} = n_{E_2}$ and $\hat{\phi} \circ \phi = n_{E_1}$, where $n = \deg \phi = \deg \hat{\phi}$. For $E_1 = E_2 = E$ we write $\bar{\phi} = \hat{\phi}$; then $\phi \circ \bar{\phi} = \bar{\phi} \circ \phi = n_E$.

Using this one can show that there are only three essentially different types of rings occurring as endomorphism rings of elliptic curves.

(3.9) Theorem. For every elliptic curve $\mathrm{End}_K(E)$ is isomorphic to either

(i) $\mathbb{Z}$, or

(ii) an order in (the ring of integers of) a complex quadratic extension of $\mathbb{Q}$, or

(iii) a maximal order in a certain totally definite quaternion algebra over $\mathbb{Q}$.

(cf. [DEUR].) □

(3.10) Remarks. Notice that $\mathrm{End}_K(E)$ depends on K : it may be that only over some extension of K all endomorphisms of E are defined. (Take for instance $A \in \mathbb{Z}$ in example (3.6) and E defined over $\mathbb{Q}$; in that case i_E is not defined over the ground field.)
The rings in (3.9)(iii) are non-commutative of $\mathbb{Z}$-rank four; they can only occur in positive characteristics. An elliptic curve is called *supersingular* whenever its ring of endomorphisms over some algebraic closure $\bar{K}$ of K is non-commutative.

An immediate consequence of this characterization of endomorphism rings is that any endomorphism $\phi \notin \mathbb{Z}$ can be identified with an integral element in an imaginary quadratic extension of $\mathbb{Q}$, so we can embed $\mathbb{Z}[\phi]$ in $\mathbb{C}$ (which is just what we did in examples (3.6) and (3.7)). In this embedding the dual $\bar{\phi}$ of ϕ corresponds to the complex conjugate $\bar{\phi}$ of the quadratic integer ϕ (whence the notation); the *norm* $N\phi = \phi\bar{\phi} \in \mathbb{Z}$ then equals the degree $\deg \phi$, as we saw before (3.9), and the *trace* of an endomorphism is defined by $\mathrm{Tr}\,\phi = \phi + \bar{\phi} \in \mathbb{Z}$.

We are now able to formulate the theorem on kernel and image of multiplication by n on a curve E ; here $E(K)[n]$ will denote the n-torsion subgroup of E over K , i.e. points defined over K of order dividing n .

(3.11) Theorem. Let the elliptic curve E be defined over some algebraically closed field $\bar{K}$. Then for any integer m , $E(\bar{K})$ is m-divisible, and

if $(\mathrm{char}\,\bar{K}, m) = 1$ then $E(\bar{K})[m] \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$

if $\mathrm{char}\,\bar{K} = p$, $m = p^k$ then $E(\bar{K})[m] \simeq \begin{cases} \mathbb{Z}/m\mathbb{Z} & \text{if } E \text{ not supersingular} \\ 0 & \text{if } E \text{ is supersingular} \end{cases}$

([TATE]p.185). □

Weierstrass models (1.4) for an elliptic curve are only unique upto transformations of the form

(3.12) $X = u^2X' + r$, $Y = u^3Y' + su^2X' + t$

which means in characteristic $\neq 2,3$ that two models of the form (1.5):

$$Y^2Z = X^3 + aXZ^2 + bZ^3 \quad \text{and}$$

$$Y^2Z = X^3 + a'XZ^2 + b'Z^3 \quad \text{over } K$$

determine the same curve if and only if there exists a $u \in K^*$ such that

$$u^4a' = a \quad \text{and} \quad u^6b' = b \ .$$

This implies that $u^{12}\Delta' = \Delta$. We see that neither Weierstrass models nor discriminants are invariant under isomorphisms.

(3.13) Definition. For an elliptic curve given by a Weierstrass equation

$$E: \ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

the *modular invariant* j is defined by

$$j(E) = j = \frac{1}{\Delta}((a_1^2+4a_2)^2 - 24(a_1a_3+2a_4))^3 \ .$$

In characteristics $\neq 2,3$ this reduces to

$$j = \frac{(-48a)^3}{-16(4a^3+27b^2)} \quad \text{with } a \text{ and } b \text{ as in (1.5)} \ .$$

(3.14) Corollary. Over an algebraically closed field $\bar{K}$ we have for elliptic curves E and E' :

$$E \text{ and } E' \text{ isomorphic} \iff j(E) = j(E') \ .$$

Furthermore, if $\mathrm{char}\,\bar{K} \neq 2,3$ then one can prove:

$$j = 0 \iff a = 0 \iff \mathrm{Aut}_{\bar{K}}(E) \simeq \mu_6$$

$$j = 1728 \iff b = 0 \iff \mathrm{Aut}_{\overline{K}}(E) \simeq \mu_4$$

$$0 \neq j \neq 1728 \iff a \neq 0 \neq b \iff \mathrm{Aut}_{\overline{K}}(E) \simeq \mu_2$$

with μ_k the group of k^{th} roots of unity (cf. [SCHO],[DEUR]). □

The special role for the values 0 and 1728 for j can also been seen in connection with supersingularity.

<u>(3.15) Proposition.</u> Let E have coefficients in the finite field $\mathbb{F}_q$ of characteristic p . Then

if $p = 2$ or 3 : E is supersingular $\iff$ $j = 0 = 1728$

if $p \geq 5$:

E with $j(E) = 0$ not supersingular $\iff p \equiv 1 \bmod 3 \iff \mathrm{End}_{\overline{\mathbb{F}}_q}(E) = \mathbb{Z}[\rho]$

E with $j(E) = 1728$ not supersingular $\iff p \equiv 1 \bmod 4 \iff \mathrm{End}_{\overline{\mathbb{F}}_q}(E) = \mathbb{Z}[i]$

and there are $\left[\frac{p}{12}\right]$ values different from 0 and 1728 which are supersingular ([TATE]p.184,185). □

§4. Finite ground field.

As we saw in example (3.8) the group of points of any elliptic curve over a finite field $\mathbb{F}_q$ is just the kernel of the endomorphism $\mathrm{Frob} - 1$ on the algebraic closure $\overline{\mathbb{F}}_q$. But since Frob is purely inseparable and since we observed (after (3.2)) that the inseparable endomorphisms (plus zero map 0_E) constitute an ideal, $\mathrm{Frob} - 1$ is separable and therefore we can find the number of points on E defined over $\mathbb{F}_q$ using (3.1):

$$\begin{aligned}\#E(\mathbb{F}_q) &= \#\ker(\mathrm{Frob} - 1) \text{ on } \overline{\mathbb{F}}_q \\ &= \deg(\mathrm{Frob} - 1) = (\phi - 1)(\bar{\phi} - 1) \\ &= N\phi + 1 - \mathrm{Tr}\,\phi = q + 1 - \mathrm{Tr}\,\phi\end{aligned}$$

where we identified Frob with a quadratic integer ϕ as in (3.10), with $|\phi| = \sqrt{q}$. This immediately gives the following theorem.

<u>(4.1) Theorem.</u> For any elliptic curve E defined over $\mathbb{F}_q$, and for any integer $m \geq 1$ we have

$$\#E(\mathbb{F}_{q^m}) = q^m + 1 - \mathrm{Tr}\,(\phi^m) \quad . \qquad \square$$

<u>(4.2) Remarks.</u> We see that $\#E(\mathbb{F}_{q^m})$ differs at most $2\sqrt{q^m}$ from $q^m + 1$, the number of points of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$; this is in fact the special case of genus 1 of the Riemann-hypothesis for function fields of curves over finite fields.

Notice that multiplying ϕ with a unit (composing the Frobenius with an automorphism) does not change $|\phi|$, but that it might affect $\mathrm{Tr}\,\phi$. Therefore it will sometimes be necessary to determine ϕ uniquely as a quadratic integer.

<u>(4.3) Reduction.</u> Much of the importance of the finite ground field case arises from the possibility of *reducing* elliptic curves: given an elliptic curve with coefficients in $\mathbb{Z}$ (or in any ring of integers A of a

number field) we can investigate solutions to the reduced equation

(4.4) $\qquad Y^2Z \equiv X^3 + aXZ^2 + bZ^3 \mod p$

for any prime ideal p (not dividing 2 or 3) of $\mathbb{Z}$ (resp. A). In other words, we are looking for the finitely many points over the finite residue class field $\mathbb{F}_p$ (resp. A/p) satisfying (4.4), which determines an elliptic curve provided it is non-singular, which means

$$4a^3+27b^2 \equiv \Delta \not\equiv 0 \mod p \qquad \text{(characteristic} \neq 2,3) \quad .$$

<u>(4.5) Definition.</u> An elliptic curve E with coefficients in some ring R is said to have *good reduction* at some prime ideal p of R when $E \bmod p$ is again an elliptic curve (that is, non-singular).

Next we will consider the two examples mentioned before again; first we introduce some auxiliary notations.

In the sequel E_δ and E^γ will respectively denote elliptic curves defined by the Weierstrass equations:

$$E_\delta : \; Y^2Z = X^3 - \delta XZ^2$$
$$E^\gamma : \; Y^2Z = X^3 + \gamma Z^3$$

with γ and δ in the ground ring or field.

<u>(4.6) Definition.</u> Let $\alpha, \pi \in \mathbb{Z}[i]$, π prime, with $(2\alpha,\pi) = 1$. The *biquadratic residue symbol* with respect to π is defined by

$$\left(\frac{\alpha}{\pi}\right)_4 = i^k \equiv \alpha^{\frac{N\pi - 1}{4}} \mod \pi \quad .$$

When extended by multiplicativity to non-prime $\nu \in \mathbb{Z}[i]$, we get for every ν with $(\nu,2) = 1$ a character of order dividing 4.

For sake of simplicity we introduce a standard normalization on elements of $\mathbb{Z}[i]$.

<u>(4.7) Definition.</u> An element $\nu \in \mathbb{Z}[i], \nu \neq 0$ is called *normalized* if

$$\nu \equiv 1 \mod 2+2i \quad .$$

For every non-unit $\nu \in \mathbb{Z}[i]$, with $1+i \nmid \nu$ this definition picks exactly one out of the four associated generators for (ν) as a principal ideal. For prime elements $\pi \nmid 2$ we have that if π is a rational prime, then $-\pi$ is normalized, and for arbitrary primes $\pi = a+bi$ is normalized $\Longleftrightarrow$ $a \equiv 3$, $b \equiv 2 \bmod 4$ or $a \equiv 1$, $b \equiv 0 \bmod 4$.

(4.8) Example. The curve E_δ .

We consider the curve E_δ for arbitrary $\delta \in \mathbb{Z}[i]$, $\delta \neq 0$. For every prime $\pi \in \mathbb{Z}[i]$, with $(2\delta,\pi) = 1$, reduction modulo π yields an elliptic curve $E_\delta \bmod \pi$ over the finite field of $N\pi$ elements. By way of example we will compute the number of points of $E_\delta \bmod \pi$ (which we will also denote by E_δ if no confusion will arise), making use only of some elementary properties of Jacobi sums (see [HA-DA],[IR-RO]Ch.VIII, IX, XVIII).

We assume our prime π to be normalized, and we identify $\mathbb{Z}[i]/(\pi) \simeq \mathbb{F}_q$ so we consider $i \bmod \pi$ and $\delta \bmod \pi$ to be elements of $\mathbb{F}_q$, the finite field of

$$\pi\bar{\pi} = \begin{cases} p \equiv 1 \bmod 4 , & p \text{ prime} \\ p^2 \equiv 1 \bmod 4 , & p \equiv 3 \bmod 4 , \ p \text{ prime} \end{cases} \qquad \text{elements.}$$

Since there is only one point at infinity $(0:1:0)$ on $E_\delta \bmod \pi$ we have

$$\#E_\delta(\mathbb{F}_q) = 1 + N_q(Y^2 = X^3 - \delta X)$$

where N_q denotes the number of solutions in $\mathbb{F}_q$.

Next we bring E_δ onto diagonal form: define

$$U = 2X - \frac{Y^2}{X^2} \quad , \quad V = \frac{Y}{X}$$

so
$$X = \frac{U + V^2}{2} \quad , \quad Y = V\,\frac{(U + V^2)}{2}$$

Then there can easily be seen to be a bijection between

$$\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q : y^2 = x^3 - \delta x\} \setminus \{(0,0)\} \qquad \text{and}$$
$$\{(u,v) \in \mathbb{F}_q \times \mathbb{F}_q : u^2 = v^4 + 4\delta\}$$

so

$$\#E_\delta(\mathbb{F}_q) = 2 + N_q(U^2 = V^4 + 4\delta) \ .$$

This is where the Jacobi sums come in:

$$N_q(U^2 = V^4 + 4\delta) = \sum_{r+s=4\delta} N_q(U^2 = r)\, N_q(V^4 = -s)$$

$$= \sum_{r+s=4\delta} \sum_{\chi^2=\chi_0} \chi(r) \sum_{\psi^4=\chi_0} \psi(-s)$$

summing over r,s in $\mathbb{F}_q$ and over multiplicative characters χ,ψ on $\mathbb{F}_q$ with χ_0 the trivial character

$$= \sum_{\chi^2=\chi=\psi^4} \sum_{r+s=4\delta} \chi(r)\,\psi(-s)$$

$$= \sum_{\chi^2=\chi=\psi^4} \chi\psi(4\delta)\,\psi(-1)\,J(\chi,\psi) \quad .$$

But for the Jacobi sums $J(\chi,\psi)$ we use ([IR-RO]Ch.VIII)

$$J(\chi_0,\chi_0) = q$$

$$J(\chi,\chi_0) = J(\chi_0,\chi) = 0 \quad \text{for } \chi \neq \chi_0$$

and $J(\chi,\chi) = J(\chi,\chi^{-1}) = -\chi(-1) = -1$ for $\chi \neq \chi_0$ with $\chi^2 = \chi_0$ since $q \equiv 1 \bmod 4$, so we are left with

$$J(\chi,\psi) \qquad \chi^2 = \chi_0 \neq \chi \quad \text{and} \quad \psi^4 = \chi_0 \neq \psi^2 \ .$$

But $\displaystyle J(\chi,\psi) = \sum_{u+v=1} \chi(u)\,\psi(v) = \sum_{u+v=1} N_q(t^2 = u)\,\psi(v)$

$$= \sum_t \psi(1-t^2) = \psi(4) \sum_t \psi\left(\frac{1+t}{2}\right) \psi\left(\frac{1-t}{2}\right)$$

$$= \psi(4)\, J(\psi,\psi)$$

and $\displaystyle J(\psi,\psi) = \sum_t \psi(t)\,\psi(1-t)$

$$= 2\sum_s \psi(s)\,\psi(1-s) \quad + \psi(\tfrac{1}{2})^2$$

where t runs over $\mathbb{F}_q$ and s runs through an appropriate half representative system of $\mathbb{F}_q$: $\bigcup_s \{s, 1-s\} = \mathbb{F}_q$.

$$\equiv \frac{q-3}{2}\cdot 2 \; + \; \psi(-1) \qquad \text{mod } (2+2i)$$

since every unit $\psi(s)\,\psi(1-s) \equiv 1 \bmod (1+i)$ and since

$$\psi(\tfrac{1}{2})^2 = \psi(2)^{-2} = \psi(2)^2 = \psi(-i(1+i)^2)^2 = \psi(-1) \ .$$

Because $\psi(-1) = \pm 1$ (depending on $q \equiv 1$ or $5 \bmod 8$), we find

(4.9) $\psi(-1)\,J(\psi,\psi) \equiv -1 \mod (2+2i)$.

Furthermore for every ψ with $\psi^2 \neq \chi_0$ on $\mathbb{F}_q$

(4.10) $|J(\psi,\psi)| = \sqrt{q}$ ([IR-RO]§8.3) .

Now we take for ψ the biquadratic residue character $\left(\frac{\cdot}{\pi}\right)_4$, in which case $\chi\psi = \psi^3 = \psi^{-1} = \bar{\psi} = \overline{\left(\frac{\cdot}{\pi}\right)_4}$ and

(4.11) $J(\psi,\psi) \equiv \sum_t t^{\frac{q-1}{4}} (1-t)^{\frac{q-1}{4}} \equiv 0 \mod \pi$ (summing over $\mathbb{F}_q$) .

Combining (4.9), (4.10) and (4.11) with π being normalized, we get

(4.12) $-\psi(-1)\,J(\psi,\psi) = \pi$.

Putting everything together we see

$$\begin{aligned}\#E_\delta(\mathbb{F}_q) &= 2 + q - 1 + \chi\psi(4\delta)\,\psi(-1)\,\psi(4)\,(-\psi(-1)\pi) + \\ &\quad + \chi\bar{\psi}(4\delta)\,\bar{\psi}(-1)\,\bar{\psi}(4)\,(-\bar{\psi}(-1)\bar{\pi}) \\ &= q + 1 - \bar{\psi}(\delta)\pi - \psi(\delta)\bar{\pi} .\end{aligned}$$

<u>(4.13) Theorem</u>. Let π be a normalized prime in $\mathbb{Z}[i]$, $0 \neq \delta \in \mathbb{Z}[i]$, with $(2\delta,\pi) = 1$ and $N\pi = q$. Then

$$\#E_\delta(\mathbb{F}_q) = q + 1 - \mathrm{Tr}\left(\overline{\left(\frac{\delta}{\pi}\right)_4}\,\pi\right) . \qquad \square$$

<u>(4.14) Corollary</u>.

$$\#E_\delta(\mathbb{F}_{q^k}) = q^k + 1 - \mathrm{Tr}\left(\left(\overline{\left(\frac{\delta}{\pi}\right)_4}\,\pi\right)^k\right) \quad \text{for all } k \geq 1 .$$

<u>Proof</u>. From (4.13) we see that the Frobenius corresponds to $\overline{\left(\frac{\delta}{\pi}\right)}\pi$ or its conjugate; the result follows by (4.1) . $\square$

<u>(4.15) Example</u>. As very first numerical example, let $\delta = 1$, $(\pi) = (3)$. Then according to (4.14) the curve $Y^2Z = X^3 - XZ^2$ should have 16 points defined over $\mathbb{F}_q$. Indeed a short computation yields:

(0 : 1 : 0)	(0 : 0 : 1)	(1 : 0 : 1)	(2 : 0 : 1)
	(i : 1+2i : 1)	(1+i : 1+2i : 1)	(2+i : 1+2i : 1)
	(i : 2+i : 1)	(1+i : 2+i : 1)	(2+i : 2+i : 1)
	(2i : 1+i : 1)	(1+2i : 1+i : 1)	(2+2i : 1+i : 1)
	(2i : 2+2i : 1)	(1+2i : 2+2i : 1)	(2+2i : 2+2i : 1)

Notice that in this example the curve was defined over $\mathbb{Z}$ already, and that reduction modulo the rational prime 3 would have given $E_\delta(\mathbb{F}_3)$. Apparently $\#E_\delta(\mathbb{F}_3) = 4$. But this can easily be derived from (4.13) in general: let $\delta \in \mathbb{Z}$ and p a rational prime. If $p \equiv 1 \bmod 4$ then (4.13) applies immediately to find $\#E_\delta(\mathbb{F}_p)$; if $p \equiv 3 \bmod 4$ then (4.13) yields $\#E_\delta(\mathbb{F}_{p^2}) = p^2 + 1 - \mathrm{Tr}(-p)$ from which we deduce by (4.1) that $\phi^2 = -p$: we find that the Frobenius is purely imaginary, and the following result for the prime field is proved. (Of course it can also be proved directly, using in the above Jacobi sum computations that in this case every square in the field is a fourth power.)

(4.16) Corollary. If $\delta \in \mathbb{Z}$, $\delta \neq 0$, $p \equiv 3 \bmod 4$ prime, then

$$\#E_\delta(\mathbb{F}_p) = p+1 .$$

Next we summarize the corresponding results for E^γ. We fix $\rho = \frac{-1+\sqrt{-3}}{2}$.

(4.17) Definition. The *sixth power residue symbol* is defined as follows: for every prime $\pi \in \mathbb{Z}[\rho]$ and every $\alpha \in \mathbb{Z}[\rho]$ with $(6\alpha, \pi) = 1$,

$$\left(\frac{\alpha}{\pi}\right)_6 = \rho^k \equiv \alpha^{\frac{N\pi-1}{6}} \bmod \pi$$

which gives by multiplicativity for every μ with $(6,\mu) = 1$ a character $\left(\frac{\cdot}{\mu}\right)_6$ of order dividing 6.

(4.18) Definition. An element $\mu \in \mathbb{Z}[\rho]$ is called *normalized* if

$$\mu \equiv 1 \bmod 2\cdot(1-\rho) .$$

Again, the images of all units are different, and we choose one out of the six associates of each element in $\mathbb{Z}[\rho]$ for which $(2\cdot(1-\rho), \mu) = 1$. For prime elements $\pi \neq 2, 1-\rho$ one finds that if π is a rational prime $p \equiv 2 \bmod 3$, then $-\pi$ is normalized, and if $\pi = a+b \notin \mathbb{Z}$ then it is normalized $\iff$ $a \equiv 5, b \equiv 2 \bmod 6$ or $a \equiv 3, b \equiv 4 \bmod 6$.

Considerations analogous to that in $\mathbb{Z}[i]$ above (compare [HA-DA], [IR-RO]§18.3) then lead to the following.

(4.19) Theorem. Let π be a normalized prime in $\mathbb{Z}[\rho]$, $0 \neq \gamma \in \mathbb{Z}[\rho]$ with $(6\gamma, \pi) = 1$, and $N\pi = q$. Then

$$\#E^{\gamma}(\mathbb{F}_q) = q + 1 - \mathrm{Tr}(\overline{\left(\frac{\gamma}{\pi}\right)_6 \pi}) \quad . \qquad \square$$

(4.20) Corollary.

$$\#E^{\gamma}(\mathbb{F}_{q^k}) = q^k + 1 - \mathrm{Tr}((\overline{\left(\frac{\gamma}{\pi}\right)_6 \pi})^k) \qquad \text{for all } k \geq 1 \ . \qquad \square$$

(4.21) Corollary. If $0 \neq \gamma \in \mathbb{Z}$ and π is a rational (normalized) prime so $-\pi = p \equiv 2 \bmod 3$, then

$$\#E^{\gamma}(\mathbb{F}_p) = p + 1 \quad . \qquad \square$$

(4.22) Remark. In the above we several times stated that the Frobenius corresponds to a certain associate of π where the unit is determined by a power residue symbol; we did not check yet however that the Frobenius is in the image of $\mathbb{Z}[i]$ resp. of $\mathbb{Z}[\rho]$ under the embedding of $\mathbb{Z}[i]$, $\mathbb{Z}[\rho]$ in $\mathrm{End}_{\overline{\mathbb{F}}_q}(E)$ i.e. that the product of i_E (resp. ρ_E) and the Frobenius makes sense in $\mathbb{Z}[i]$ or $\mathbb{Z}[\rho]$. However (working this out only for E_δ, the other case is similar), for $p \equiv 1 \bmod 4$ this is clear from proposition (3.15), while for $p \equiv 3 \bmod 4$ it is a consequence of corollary (4.16) - which we therefore have to proof directly as indicated - that the Frobenius is even an element of $\mathbb{Z}$.

This means that we now have completely determined the number of points on each of the E_δ, E^γ over any finite field. In doing so we determined the Frobenius endomorphism upto complex conjugation. In order to find the *structure* of $E_\delta(\mathbb{F}_q)$ and $E^\gamma(\mathbb{F}_q)$ - not only as a group, but even as a $\mathbb{Z}[i]$ resp. $\mathbb{Z}[\rho]$ module - we first determine the Frobenius unambiguously.

(4.23) Proposition. Let π be a normalized prime in $\mathbb{Z}[i]$. Then for $\delta \in \mathbb{Z}[i]$ with $(2\delta,\pi)=1$, the Frobenius endomorphism belonging to $E_\delta \bmod \pi$ corresponds to $\overline{\left(\frac{\delta}{\pi}\right)_4} \cdot \pi$ in $\mathbb{Z}[i]$.
If π' is a normalized prime in $\mathbb{Z}[\rho]$ and $0 \neq \gamma \in \mathbb{Z}[\rho]$, then for γ with $(6\gamma,\pi')=1$ the Frobenius of $E^\gamma \bmod \pi'$ is given by $\overline{\left(\frac{\gamma}{\pi'}\right)_6} \cdot \pi'$ in $\mathbb{Z}[\rho]$.

Proof. We only give the proof for the curve E_δ, the other case can be dealt with analogously.
From theorems (4.13) and (4.1) it follows, as mentioned above, that the Frobenius is either the element indicated in the proposition or its complex conjugate. We consider two cases.
Let first the primes π and $\bar{\pi}$ be non-associated, i.e. $\pi \cdot \bar{\pi} = p \equiv 1 \bmod 4$ p prime. We identified $\mathbb{Z}[i]/\pi$ and $\mathbb{F}_p$; but we also have a map $\mathbb{Z}[i] \to \mathbb{F}_p$ defined by the action on the tangent spaces, as in (3.2), since $\mathbb{Z}[i]$ injects into $\mathrm{End}_{\mathbb{F}_p}(E_\delta)$. By making use of the invariant differential $\frac{dx}{y}$ we verify that the diagram

$$\begin{array}{ccc} \mathbb{Z}[i] & \longrightarrow & \mathrm{End}_{\mathbb{F}_p}(E_\delta) \\ & {\scriptstyle \bmod \pi} \searrow \quad \swarrow & \\ & \mathbb{F}_p & \end{array}$$

commutes, i.e. that we made the right choice for the action i_E in (3.6):

$$\frac{d(i_E(x))}{i_E(y)} = \frac{d(-x)}{iy} = i\,\frac{dx}{y}$$

so "taking differentials commutes with multiplication by i".
Since we know that $\mathrm{Frob} \in (\pi)$ or $(\bar{\pi})$, and since we know that in the above diagram on the one hand π is mapped to 0 but $\bar{\pi}$ is not, while on the other hand the Frobenius is mapped to zero because it is inseparable, we can conclude that $\mathrm{Frob} \in (\pi)$. That settles the first case.

In the other case, when $(\pi) = (\bar{\pi})$ this argument clearly does not work. But here we observe that in some instances the case is already settled, namely when $\overline{\left(\frac{\delta}{\pi}\right)_4} = \pm 1$. For then $\overline{\left(\frac{\delta}{\pi}\right)_4}\pi = \left(\frac{\delta}{\bar{\pi}}\right)_4\bar{\pi}$ and we are done.

But the remaining cases can be deduced from this by "twisting", as follows. Let E_1 be the curve $Y^2Z = X^3 - XZ^2$ of which we know that the Frobenius (denoted by ϕ_1) corresponds to the normalized prime $\pi = \overline{\left(\frac{\delta}{\pi}\right)_4}\pi = \left(\frac{\delta}{\bar{\pi}}\right)_4\bar{\pi} = \bar{\pi}$, and let E_δ be given for some $\delta \in \mathbb{F}_q^*$ $q = N\pi$. Then over the algebraic closure $\overline{\mathbb{F}}_q$ we find an isomorphism (in fact of course already over some finite extension) $E_1 \xrightarrow{\sim} E_\delta$ for instance given by:

$$(x : y : z) \longmapsto (\sqrt[4]{\delta}^2 x : \sqrt[4]{\delta}^3 y : z) \quad .$$

We thus see that $E_1(\overline{\mathbb{F}}_q) \simeq E_\delta(\overline{\mathbb{F}}_q)$; but then this isomorphism should induce an isomorphism on the endomorphism ring that is the identity on the subring $\mathbb{Z}[i]$ if we define the action on E of i as in (3.6) by $i_E(x : y : z) = (-x : iy : z)$. Now

$$\phi_1(P) = \phi_1(\ (\sqrt[4]{\delta}^2 x : \sqrt[4]{\delta}^3 y : z)\ ) = (\sqrt[4]{\delta}^2 x^q : \sqrt[4]{\delta}^3 y^q : z^q)$$

while

$$\phi_\delta(P) = \phi_\delta(\ (\sqrt[4]{\delta}^2 x : \sqrt[4]{\delta}^3 y : z)\ ) = ((\sqrt[4]{\delta}^2)^q x^q : (\sqrt[4]{\delta}^3)^q y^q : z^q)$$

which means that modulo π the difference is given by multiplication by a unit, namely,

$$(\sqrt[4]{\delta}^3)^{q-1} = (\delta^3)^{\frac{q-1}{4}} \equiv \bar{\delta}^{\frac{q-1}{4}} \mod \pi$$

and

$$(\sqrt[4]{\delta}^2)^{q-1} = (\delta^2)^{\frac{q-1}{4}} \equiv \bar{\delta}^{2\frac{q-1}{4}} \mod \pi$$

so $$\phi_\delta(P) = \overline{\left(\frac{\delta}{\pi}\right)_4} \cdot \phi_1(P)$$

where the residue symbol denotes complex multiplication on E_1 with the unit it determines.

Since ϕ_1 corresponds to π , this ends the proof of (4.22). □

We now know that under the proper normalizations $E_\delta \bmod \pi$ is annihilated by $\text{Frob} - 1 = \pi - 1$; but we can prove that this is precisely the annihilator, that is we have the following proposition, which could be called an analogue of $(\mathbb{Z}/p\mathbb{Z})^* \simeq (\mathbb{Z}/(p-1)\mathbb{Z})$.

(4.24) Proposition. Let π be prime in $\mathbb{Z}[i]$ and δ such that $(2\delta,\pi)=1$. If we normalize π by $\pi \equiv \overline{\left(\frac{\delta}{\pi}\right)_4} \bmod 2+2i$ then (with $q = N\pi$)

$$E_\delta(\mathbb{F}_q) \simeq \mathbb{Z}[i]/(\pi-1) \quad \text{as} \quad \mathbb{Z}[i]\text{-modules.}$$

The proof is a consequence of the following lemma.

(4.25) Lemma. Let R be a principal ideal domain having only finite residue class fields. For every finite R-module M :
if $\#\{x \in M : (b)x = 0\} \le \#R/(b)$ for every ideal $0 \ne (b) \subset R$,
then M is a cyclic module: $M \simeq R/(a)$, for some $(a) \subset R$.

Proof. If M is not cyclic, then by the structure theorem for finitely generated torsion modules over principal ideal domains ([LANG]2 Ch.XV) it is the sum of at least 2 cyclic modules: $M = \bigoplus_{i=1}^{k} R/(a_i)$ which can be chosen such that $(a_{i+1}) \mid (a_i)$. Then at least one prime ideal (π) divides both (a_1) and (a_2) ; this (π) contradicts the assumption. □

Proof of (4.24). We know that $E_\delta(\mathbb{F}_q)$ is a finite $\mathbb{Z}[i]$-module (annihilated by $\pi-1$). Now for $0 \ne \alpha = \mathbb{Z}[i]$ we have

$$\#\{P \in E_\delta(\mathbb{F}_q) : \alpha . P = 0_E\} \le \{P \in E_\delta(\overline{\mathbb{F}}_q) : \alpha \cdot P = 0_E\} \le \alpha \cdot \bar{\alpha} = N\alpha = \#\mathbb{Z}[i]/(\alpha)$$

so application of (4.25) yields the desired conclusion. □

We find a similar result for E^γ.

(4.26) Proposition. Let π be prime in $\mathbb{Z}[\rho]$ and γ such that $(6\gamma,\pi)=1$. If we normalize π by $\pi \equiv \overline{\left(\frac{\gamma}{\pi}\right)_6} \bmod 2(1-\rho)$ then (with $q = N\pi$)

$$E^\gamma(\mathbb{F}_q) \simeq \mathbb{Z}[\rho]/(\pi-1) \quad \text{as} \quad \mathbb{Z}[\rho]\text{-modules.} \qquad \square$$

§5. Elliptic curves over Artin rings.

As pointed out in the introduction, and as we will see in the next chapter, we want to work with reductions of elliptic curves by ideals that are not necessarily maximal. Therefore we need to define elliptic curves over a wider class of rings than fields. Since in our applications we will only encounter $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}[i]$ or $\mathbb{Z}[\rho]$ modulo (ν) as ground rings, we will confine ourselves for simplicity to Artin rings.
(All rings are assumed to be commutative with 1).

(5.1) Remark. We briefly recall the basic properties of Artin rings (see [A-McD]Ch.VIII). By definition an Artin ring is a ring that satisfies the descending chain condition on ideals. This is equivalent to A being noetherian of dimension 0 (i.e. every prime ideal is maximal). Furthermore any Artin ring has only finitely many maximal ideals $\mathfrak{m}_i$ $(i=1,\dots,n)$, and there is a $k>0$ such that $\prod_{i=1}^{n} \mathfrak{m}_i^k = 0$. The structure theorem for Artin rings then says that $A \xrightarrow{\sim} \prod_{i=1}^{n} A/\mathfrak{m}_i \approx A_{\mathfrak{m}_i}$ now gives an (upto isomorphism) unique decomposition of A into a finite direct product of local Artin rings.

(5.2) Definition. An *elliptic curve over an Artin ring* A is the set of projective points

$$E(A) = \{(x:y:z)\ ,\ x,y,z \in A\ ,\ (x,y,z) = (1) \text{ and } F(x,y,z) = 0\}$$

satisfying the homogeneous Weierstrass form $F \in A[X,Y,Z]$ with $\Delta \in A^*$, equipped with the structure of an abelian group under addition defined below.
Here of course $(x_1:y_1:z_1) = (x_2:y_2:z_2) \iff \exists u \in A^*$ such that $(x_1,y_1,z_1) = (ux_2,uy_2,uz_2)$.

(5.3) Addition. First we define addition of points on elliptic curves over local (Artin) rings as follows. We make use of the formulas of assertion (2.8). Let $P_1,P_2 \in E(A_{\mathfrak{m}})$; find an i $(1 \le i \le k)$ for which

$$T_i(x_1,y_1,z_1,x_2,y_2,z_2) \not\equiv 0 \bmod m$$

and now define with this i :

$$P_1 + P_2 = (Q_i(x_1,\dots,z_2) : R_i(x_1,\dots,z_2) : S_i(x_1,\dots,z_2)) .$$

For arbitrary Artin rings we then extend this definition by multiplicativity making use of the structure theorem:

$$E(A) = E(\prod_{i=1}^{n} A_{m_i}) = \prod_{i=1}^{n} E(A_{m_i}) .$$

(5.4) Verifications. Let us verify that this definition makes sense. The existence of at least one i satisfying $T_i \not\equiv 0 \bmod m$ in A_m is guaranteed by (2.8) , A_m/m being a field.

That $P_1 + P_2 \in E(A_m)$ is clear since by (2.21) the coordinates satisfy the required Weierstrass equation, while they can not all reduce to zero as can be seen immediately from commutativity of the diagram

$$\begin{array}{ccc} E(A_m) \times E(A_m) & \xrightarrow{+} & E(A_m) \cup (0:0:0) \\ \downarrow & & \downarrow \\ E(A_m/m) \times E(A_m/m) & \xrightarrow{+} & E(A_m/m) \end{array}$$

(in which vertical arrows denote reduction of coordinates modulo m) and the fact that addition on $E(A_m/m)$ is well-defined.

The sum is independent of the choice of i : this follows from (2.22). The other axioms for a commutative group are clearly satisfied except for associativity, which is guaranteed by (2.24).

(5.5) Example. With this definition we can now reduce the curve

$$E_\delta : \; Y^2Z = X^3 - \delta XZ^2 , \qquad \mathbb{Z}[i] ,$$

modulo any non-unit ν for which $(2\delta,\nu) = 1$, instead of only prime elements. Since we defined these reductions multiplicatively, it suffices to consider $E_\delta \bmod \pi^k$ for π prime, $(2\delta,\pi) = 1$ and $k \geq 2$; the case $k = 1$ was treated in example (4.8). We suppose that our prime is normalized by $\pi \equiv \overline{\left(\frac{\delta}{\pi}\right)_4} \bmod 2+2i$.

Denoting by A_k (for $k \geq 1$) the ring $\mathbb{Z}[i]/(\pi^k)$ and by I_k the ideal (π^{k-1}) of A_k , we get for every $k \geq 2$, by reduction of the coordinates modulo π^{k-1} :

$$r_k : \quad E_\delta(A_k) \longrightarrow E_\delta(A_{k-1}) = E_\delta(A_k/I_k) \quad ,$$

a group homomorphism (by definitions (5.2) and (5.3)).

These reductions are surjective, since any point on $E\,(A_k/I_k)$ can be lifted using Hensel's lemma; moreover, the kernel of r_k can be seen to be isomorphic to the additive group I_k^+ by a change of variable. For,

if $\quad r_k(x : y : z) = (0 : 1 : 0)$

then $\pi \nmid y$ but $\pi^{k-1} | x$ and $\pi^{k-1} | z$.

From Weierstrass equation (1.5) we can see in general that

$$\pi | z \quad \Rightarrow \quad \pi | x \quad \text{and if} \quad \pi^m | x \text{ say, then } \pi^{3m} | z \quad .$$

So in the kernel of r_k we may write $(x : y : z) = (-\frac{x}{y} : -1 : -\frac{z}{y})$ and now the mapping $w \longmapsto (w : -1 : 0)$

$$I_k^+ \longrightarrow \ker(r_k)$$

gives a bijection that is not only a group homomorphism, but even a $\mathbb{Z}[i]$-module homomorphism (see for this [TATE]§3).

This implies that multiplication by π on $E_\delta(A_k)$ sends all points to the zero element of $E_\delta(A_{k-1})$.

(5.6) Corollary. For any prime π in $\mathbb{Z}[i]$, normalized by $\pi \equiv \overline{\left(\frac{\delta}{\pi}\right)_4}$ mod 2+2i for δ with $(2\delta,\pi) = 1$ we have that $E_\delta(\mathbb{Z}[i]/(\pi^k))$ is annihilated by $(\pi - 1)\pi^{k-1}$ for any $k \geq 1$. □

(5.7) Corollary. For any prime π in $\mathbb{Z}[\rho]$, normalized by $\pi \equiv \overline{\left(\frac{\gamma}{\pi}\right)_6}$ mod $2\cdot(1-\rho)$ for γ with $(6\gamma,\pi) = 1$, $E^\gamma(\mathbb{Z}[\rho]/(\pi^k))$ is annihilated by $(\pi - 1)\pi^{k-1}$ for any $k \geq 1$. □

CHAPTER II PRIMALITY TESTS

§6. Primality testing.

In this chapter we will apply results of the previous chapter to primality testing, i.e. deciding whether a certain given positive integer n is prime or composite. To us a *primality test* will be a sufficient criterion for primality, and a *compositeness test* will be a sufficient criterion for compositeness; of course we should add that a good test is also (computationally) effective, but we will not specify this here in terms of complexity.

Since it only takes one non-trivial multiplication with outcome n to show that the integer n is composite, while primality - the *non*-existence of non-trivial divisors - can only be proved in some "indirect" way, it seems obvious at first sight that , generally speaking, recognizing composite numbers is easier than recognizing primes. However, *finding* a factor of a given large integer turns out to be even harder than proving primality. Though proving the compositeness of an integer without indicating a factor seems remarkable, the most commonly used tool for this is just Fermat's theorem

(6.1) $\quad n \text{ prime} \Rightarrow \text{ for all } a \text{ with } (a,n)=1 : \ a^{n-1} \equiv 1 \bmod n$

which gives rise to the following compositeness test :

(6.2) $\quad a^{n-1} \not\equiv 1 \bmod n \ , \ (a,n)=1 \ \Rightarrow \ n \text{ composite} .$

When sharpened to

(6.3) $\quad a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \bmod n \ , \ (a,n)=1 \ \Rightarrow \ n \text{ composite} ,$

(using Jacobi's symbol $\left(\frac{\cdot}{n}\right)$) , one can show that for every composite n at least a half of the elements a with $(a,n)=1$ yields a proof for its compositeness (see [LEHM],[SO-ST]). When trying several a does not lead to such a proof, n will probably be prime.
At that point one wants to subject n to a primality test.

The prototype for our primality tests is based on the converse of Fermat's theorem; since this does unfortunately not hold, some modifications have to be made first.

For instance, the converse of (6.3) does hold, but checking the desired congruence for all a for large n (for our purposes upto several hundreds of digits) is computationally not feasible. More useful is the following proposition, the proof of which we will discuss in (6.7), after an application.

(6.4) Proposition. Let n be an odd positive integer. If there exists an a in $\mathbb{Z}$ such that

$$(a,n) = 1 \quad \text{and} \quad a^{n-1} \equiv 1 \bmod n \quad \text{but}$$

(6.5) $$\text{for all prime numbers } q \text{ dividing } n-1 : \quad a^{\frac{n-1}{q}} \not\equiv 1 \bmod n$$

then n is prime.

(6.6) Example. Pépin's test.

This one of the older (1877) and easiest primality tests, designed especially for the Fermat numbers $n = 2^{2^k} + 1$, $k \geq 1$. It reads:

$$n = 2^{2^k} + 1 \text{ is prime} \iff 3^{\frac{n-1}{2}} \equiv -1 \bmod n$$

and is an immediate consequence of (6.3) and (6.4), observing that

$$\left(\frac{3}{n}\right) = \left(\frac{n}{3}\right) = \left(\frac{2}{3}\right) = -1 \quad \text{for} \quad k \geq 1 .$$

This way $2^{2^{14}} + 1$ was proved to be composite, though no factor is known ([BLSTW]).

The above example, and in fact the proposition itself, shows immediately the main shortcoming of these type of tests: the use of (6.5) is restricted to those n for which the prime factorization of $n-1$ is completely known. Though this may be relaxed for instance to knowledge of a partial factorization (see below), it is still true that the tests we consider are limited in the sense that they are particularly suited for integers of a *special form*.

(6.7) Proof of (6.4). The proof of (6.4) is obvious: the conditions on a imply that its order in $(\mathbb{Z}/n\mathbb{Z})^*$ equals $n-1$, which means that $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic of order $n-1$, showing that n is prime.

It is worth noticing however that what really matters here is the *exponent* of $(\mathbb{Z}/n\mathbb{Z})^*$ rather than its order: writing $n = \prod_{j=1}^{t} p_j^{k_j}$, the exponent of $(\mathbb{Z}/n\mathbb{Z})^*$ equals (n is odd)

$$\operatorname{lcm}_j \phi(p_j^{k_j}) = \operatorname{lcm}_j ((p_j-1)p_j^{k_j-1})$$

(in which ϕ denotes Euler's function). Since the order of $a \bmod n$ is $n-1$, and $(n,n-1)=1$ we find that

$$(6.8) \qquad \left(\prod_{j=1}^{t} p_j^{k_j}\right) - 1 \;\Big|\; \operatorname{lcm}(p_j-1)$$

which gives a contradiction (using that $2 \mid (p_j-1)$) unless $t=1=k_1$: n is prime.

Rephrased this way we will see that the proof lends itself for generalization as well as the proposition itself. □

(6.9) Remark. As can be seen from the proof, the uniform condition on a in (6.4) for all primes dividing $n-1$ can be replaced by a condition in which a may depend on the prime:

$$(6.10) \qquad \forall\, q \mid n-1 \ (q \text{ prime})\ \exists\, a \text{ satisfying } (a,n)=1,$$

$$a^{n-1} \equiv 1 \bmod n \quad \text{but} \quad a^{\frac{n-1}{q}} \not\equiv 1 \bmod n \quad .$$

When only a partial factorization of $n-1$ is known, considerations similar to the above lead, if not to a primality proof, at least to information on possible factors of n. This is shown by the following theorem, in which s should be thought of as the factored part of $n-1$.

(6.11) Theorem. Suppose we are given n, s in $\mathbb{Z}_{>1}$, $s \mid n-1$, and $a \in \mathbb{Z}$ with $a^{n-1} \equiv 1 \bmod n$. If for every prime q dividing s we have

$$\gcd\left(a^{\frac{n-1}{q}} - 1 , n \right) = 1$$

then every divisor r of n satisfies $r \equiv 1 \bmod s$.

<u>(6.12) Remarks</u>. For the proof we just observe here that $a^{\frac{n-1}{s}}$ has order s in $(\mathbb{Z}/p\mathbb{Z})^*$ when taken modulo the prime p , $p|n$.

It is clear that the theorem yields primality proofs when $s > \sqrt{n}$ (or, with some more caution, even if $s > \sqrt[3]{n}$: see [LENS]).

Again the uniform condition on a can be replaced by

(6.13) $\quad \forall$ prime $q|s$ $\exists$ a : $a^{n-1} \equiv 1 \bmod n$ and $\gcd\left(a^{\frac{n-1}{q}} - 1 , n \right) = 1$.

<u>(6.14) Example</u>. Let $n = h \cdot 2^k + 1$ with $1 \le h \le 2^k$. Then, if there exists an a satisfying

$$a^{\frac{n-1}{2}} \equiv -1 \bmod n$$

we conclude that n is prime.

For example: $2^{229}(2^{228} - 1) + 1$ was proved prime this way ([BLSTW]).

Primality tests based on (6.4) and (6.11) have been generalized in such a way, that also use can be made of (partial) factorizations of $n+1$, n^2+n+1 etc. ([WILL]), giving rise for example to the well-known Lucas-Lehmer test for Mersenne numbers. In the next section we will generalize the tests in a somewhat other direction; we want to replace the group structure of $(\mathbb{Z}/n\mathbb{Z})^*$ by the module structure of the group of points $E(A)$ over an Artin ring A of an elliptic curve admitting complex multiplication.

§7. The $\mathbb{Z}[i]$-tests.

In the following "generalization" of theorem (6.11) the main primality test of this section for $\mathbb{Z}[i]$ is contained.

The curve E_δ is defined as before: $Y^2Z = X^3 - \delta XZ^2$; and by $P \equiv 0_E \bmod \mu$ we will denote that $P = 0$ on the curve $E \bmod \mu$.

(7.1) Theorem. Let $\nu \in \mathbb{Z}[i]$ and let $\sigma \in \mathbb{Z}[i]$ divide $\nu - 1$.

If there exist $\delta \in \mathbb{Z}[i]$ with $(2\delta, \nu) = 1$ and points P_j on $E_\delta(\mathbb{Z}[i]/(\nu))$ satisfying:

(7.2) for all j : $(\nu - 1)\cdot P_j = 0_{E_\delta}$

and

(7.3) for every $\gamma | \sigma$,$\gamma \in \mathbb{Z}[i]$ prime, there exists a j such that:

for every non-unit $\mu \in \mathbb{Z}[i]$, $\mu | \nu$ we have $(\frac{\nu - 1}{\gamma})\cdot P_j \not\equiv 0_{E_\delta} \bmod \mu$

then every divisor ρ of ν , normalized by

$$\rho \equiv \overline{\left(\frac{\delta}{\rho}\right)_4} \bmod 2+2i \quad , \quad \text{satisfies}$$

(7.4) $\rho \equiv 1 \bmod \sigma$.

If moreover $\sigma \nmid 2$ then also

$$\nu \equiv \overline{\left(\frac{\delta}{\nu}\right)_4} \bmod 2+2i \, .$$

(7.5) Corollary. $(|\sigma| - 1)^2 > |\nu| \Rightarrow \nu$ prime in the above.□

Proof of (7.1). Choose some prime $\pi | \nu$.

Consider the points $Q_j = (\frac{\nu - 1}{\sigma})\cdot P_j$. According to (7.2) we have for all j: $\sigma Q_j = 0_{E_\delta}$, while (7.3) implies that for every prime γ dividing σ there is a j such that $\frac{\sigma}{\gamma} Q_j \not\equiv 0_{E_\delta} \bmod \pi$. We conclude from this that σ divides the annihilator of $E_\delta \bmod \pi$, which is $\pi - 1$ for π normalized as in the theorem, as we saw in (4.23). By multiplicativity this leads to the desired conclusion. □

(7.6) Remarks. It is important to note that conditions like those of (7.2) and (7.3) about the annihilation of points after reduction, that may seem elusive at first sight, can be made very explicit - and thereby suited for easy computational verification - as follows. Since we know how to add and multiply by i on E_δ, we know how to compute e.g. $Q = (\frac{\nu-1}{\gamma})\cdot P$ (we may also use explicit formulas for multiplication by m given in [CASS]); now the condition $Q \not\equiv 0_{E_\delta} \bmod \pi$ comes down to z_Q (and therefore x_Q) being not divisible by π (see §5). We thus have

$$\forall\, \mu|\nu \quad Q \not\equiv 0_{E_\delta} \bmod \mu \quad \Longleftrightarrow \quad \gcd(z_Q,\nu) = 1 \quad .$$

Notice that the normalization of ν as in the theorem here is a conclusion and not a condition; but in practice of course one first makes sure that it is satisfied for the δ under consideration. The verification of such congruences can be done using the biquadratic reciprocity laws and its supplementary laws.

If we succeed in factoring $\nu - 1$ completely in $\mathbb{Z}[i]$ we can use the following theorem.

(7.7) Theorem. Let $\nu \in \mathbb{Z}[i]$ and suppose that

(7.8) $\quad (\nu\,,\ 3\cdot5\cdot13\cdot17\cdot29) = 1$.

If there exist $\delta \in \mathbb{Z}[i]$ with $(\nu,2\delta) = 1$ and points P_j on $E_\delta(\mathbb{Z}[i]/(\nu))$ satisfying:

(7.9) $\quad \forall j:\ (\nu-1)\cdot P_j = 0_{E_\delta}$

(7.10) $\quad \forall$ prime $\gamma|\nu-1\ \ \exists j:\ (\frac{\nu-1}{\gamma})\cdot P_j \neq 0_{E_\delta}$

then ν is prime in $\mathbb{Z}[i]$

(and $\quad \nu \equiv \overline{\left(\frac{\delta}{\nu}\right)_4} \bmod 2+2i$).

Proof. By (7.9) and (7.10) $\nu - 1$ divides the annihilator of $E_\delta(\mathbb{Z}[i]/(\nu))$. But from §5 we know that this annihilator divides $\operatorname{lcm}((\pi_j - 1)\pi_j^{k_j-1})$ with $\pi_j \equiv \overline{\left(\frac{\delta}{\pi_j}\right)_4} \bmod 2+2i$ if we write $\nu' = \prod_{j=1}^{t} \pi_j^{k_j}$ where ν' denotes the associate of ν that is likewise normalized. But since $(\nu'-1,\nu) = 1$ we conclude that

(7.11) $\quad \nu' - 1 \ \big|\ \operatorname{lcm}(\pi_j - 1)$.

Now $(\nu,2) = 1$ so always $1+i \mid \pi_j$ and thus

$$(7.12) \qquad |\mathrm{lcm}(\pi_j - 1)| \le |(1+i)\prod_{j=1}^{t} \frac{\pi_j - 1}{1+i}| \le \frac{1}{\sqrt{2}^{t-1}} \prod_{j=1}^{t} |\pi_j - 1| <$$

$$< \frac{1}{\sqrt{2}^{t-1}}(\sqrt{37} + 1)^t$$

because condition (7.8) on ν implies that $|\pi_j| \ge \sqrt{37}$, and therefore also

$$(7.13) \qquad |\nu' - 1| \ge |\nu| - 1 \ge \sqrt{37}^{t} - 1 \quad .$$

For $t \ge 2$ now (7.12) and (7.13) contradict (7.11) while for $t = 1$, $k_1 \ge 2$

$$(7.14) \qquad |\nu' - 1| \ge |\nu| - 1 \ge \sqrt{37}^{k} - 1$$

together with (7.12) also contradicts (7.11). The result follows , □

<u>(7.15) Remarks</u>. Condition (7.8) that ν has no small prime factors (which in practice is no restriction of course) is put in to make the inequalities (7.12)-(7.14) work; in fact it can be relaxed to $(\nu,15) = 1$ as we will see in the next section. We will prove there that there exist only finitely many composite ν for which all conditions of the theorem, except (7.8), can be met, and that they all have $(\nu,15) > 1$.

<u>(7.16) Rational primality</u>. Let now $n > 1$ be an odd rational integer with $(n,15) = 1$. If $n \equiv 1 \bmod 4$ write $n = \nu\cdot\bar{\nu}$ in $\mathbb{Z}[i]$; if $n \equiv 3 \bmod 4$ take $n = \nu$. We next choose $\delta \in \mathbb{Z}[i]$ and normalize :

$$\nu \equiv \overline{\left(\frac{\delta}{\nu}\right)_4} \bmod 2+2i \quad .$$

Factoring $\nu - 1$ as far as possible, we get a factored $\sigma \mid \nu - 1$ and we can apply theorem (7.1) or, if we are lucky, even (7.7), trying to prove that ν and therefore n is prime.

<u>(7.17) Remarks</u>. First notice that not every $n \equiv 1 \bmod 4$ can be written as $n = \nu\cdot\bar{\nu}$ in $\mathbb{Z}[i]$; but if n is prime then this decomposition does exist, and what is more, it can be found efficiently (in "polynomial time", see eg. [SCHO]). This makes testing for primality in $\mathbb{Z}$ and $\mathbb{Z}[i]$

polynomially equivalent.

Secondly, it is important to observe here that we can make use of (partial) factorizations of the different associates of ν minus 1 (in particular when we use theorem (7.1)). What matters here is the factorization of $\nu^4 - 1 = -(\nu - 1)(-\nu - 1)(i\nu - 1)(-i\nu - 1)$; we utilize all factors of this we can find, choosing different δ's.

We also remark that knowledge of a (partial) factorization of $\nu - 1$ in $\mathbb{Z}[i]$ of course does not mean that we know that of $n - 1$ in $\mathbb{Z}$, i.e. that we could also use the classical tests (except when $n \equiv 3 \bmod 4$ and $n = \nu$ after normalization). In any case the advantage of (7.1) and (7.7) over (6.11) and (6.4) is the possibility of using different δ for the same (associate) of ν, yielding in fact a sequence of (independent) tests of the type of §6, instead of just one for every n.

§8. Pseudoprimes in $\mathbb{Z}[i]$.

This section is devoted to a curiosity: the existence of what we will call pseudoprimes in $\mathbb{Z}[i]$. For us a *pseudoprime* in general will be a composite number that passes a certain test . (Since we have understood a primality test to be a sufficient condition for primality we cannot say it passes a certain primality test.)

(8.1) Examples. A composite number $n \in \mathbb{Z}_{>1}$ is called a *pseudoprime to the base* a , for $a \in \mathbb{Z}_{>1}$, when $a^{n-1} \equiv 1 \bmod n$.

A *Carmichael number* is a composite integer that is pseudoprime to all bases:

(8.2) $\quad \forall\, a \in \mathbb{Z},\ (a,n) = 1 :\ a^{n-1} \equiv 1 \bmod n$.

Thus the Carmichael numbers (which do exist: the least is 561) are just those composites that prevent us from taking the converse of Fermat's theorem as primality test.

(8.3) Definition. We will call an element ω of $\mathbb{Z}[i]$ a *pseudoprime in* $\mathbb{Z}[i]$ whenever $1+i \nmid \omega$, it is composite and writing

(8.4) $\quad \omega = \prod_{j=1}^{t} \pi_j^{k_j}$ with π_j different prime elements in $\mathbb{Z}[i]$, $\pi_j \nmid 2$, $k_j > 0$

it satisfies

(8.5) $\quad \omega - 1 \mid \operatorname{lcm}_j (\pi_j - 1)$.

(8.6) Remarks. By definition, a pseudoprime in $\mathbb{Z}[i]$ is not just an element ω of $\mathbb{Z}[i]$, but such an element together with its decomposition (8.4); notice that this is not just the prime decomposition of ω in $\mathbb{Z}[i]$: we suppose in (8.4) that for $j \neq j'$ always $\pi_j \neq \pi_{j'}$, but it may be that $(\pi_j) = (\pi_{j'})$, i.e. that π_j and $\pi_{j'}$ are associates. The definition is of course motivated by the proof of theorem (7.8) : it may be that these composites satisfy all conditions of the statement except $(\omega, 15) = 1$ (note that in (7.8) associated primes π_j and $\pi_{j'}$ for $j \neq j'$ are ruled out by the normalizations).

Remark that the divisibility condition in $\mathbb{Z}$ can be met also: take $n = (-2)^2$, then $n-1 = 3$ divides $\text{lcm}(-3)$. Of course, under our usual (but often implicit) normalization for primes in $\mathbb{Z}$ to be positive, such "pseudoprimes" do not exist in $\mathbb{Z}$.

<u>(8.7) Theorem</u>. The only pseudoprimes in $\mathbb{Z}[i]$ are:

$$\begin{array}{lll}
\omega_1 = (-2-i)(-3)(-2+5i) & = -27+24i & \omega_2 = \bar{\omega}_1 \\
\omega_3 = (-2-i)(-2+3i)(-4-i) & = -32+9i & \omega_4 = \bar{\omega}_3 \\
\omega_5 = (-3)(-4+i)(-4-i) & = -51 & \\
\omega_6 = (-1+2i)(-2-i)(-2-3i) & = -17-6i & \omega_7 = \bar{\omega}_6
\end{array},$$

where $\bar{\ }$ denotes complex conjugation of each of the factors of ω.

<u>Proof</u>. We write $\omega = \prod_{j=1}^{t} \pi_j^{k_j}$ with $t \geq 1$, $k_j \geq 1$ and $1+i \nmid \pi_j$, and we suppose that $\omega - 1 \mid \text{lcm}(\pi_j - 1)$.

For this to hold we need at least an inequality

$$(8.8)\qquad (\prod_{j=1}^{t} |\pi_j^{k_j}|) - 1 \leq |\prod_{j=1}^{t} \pi_j^{k_j} - 1| = |\omega - 1| \leq |\text{lcm}(\pi_j - 1)| \leq$$

$$\leq |1+i| \cdot \prod_{j=1}^{t} \frac{|\pi_j - 1|}{|1+i|} = \frac{1}{\sqrt{2}^{t-1}} \prod_{j=1}^{t} |\pi_j - 1|$$

since always $1+i \mid \pi_j - 1$. This yields the necessary inequality

$$(8.9)\qquad \prod_{j=1}^{t} \frac{|\pi_j - 1|}{|\pi_j|^{k_j}} \geq \sqrt{2}^{t-1} \left(1 - \frac{1}{|\pi_j|^{k_j}}\right).$$

For finding prime elements with large quotient $\frac{|\pi - 1|}{|\pi|}$ it is convenient to use the following obvious lemma.

<u>(8.10) Lemma</u>. Let $z \in \mathbb{C}$, $z = a+bi$. Then for every $r \in \mathbb{R}_{>1}$ we have

$$\frac{|z-1|}{|z|} \geq r \iff b^2 + \left(a + \frac{1}{r^2 - 1}\right)^2 \leq \frac{1}{(1-r^2)^2}. \qquad \square$$

Using this for decreasing values of r one proves that the prime elements in $\mathbb{Z}[i]$ can be ranked in order of decreasing quotient $\frac{|\pi - 1|}{|\pi|}$ as follows.

<u>(8.11) Corollary</u>. The thirteen prime elements in $\mathbb{Z}[i]$ with largest

quotient $\frac{|\pi - 1|}{|\pi|}$ are:

π :	$-2\pm i$		-3		$-1\pm 2i$		$-3\pm 2i$		$-4\pm 2i$		$-2\pm 3i$		$-5\pm 2i$		...
$\frac{|\pi-1|}{|\pi|}$:	$\frac{\sqrt{10}}{\sqrt{5}}$	>	$\frac{4}{3}$	>	$\frac{\sqrt{8}}{\sqrt{5}}$	>	$\frac{\sqrt{13}}{\sqrt{20}}$	>	$\frac{\sqrt{26}}{\sqrt{17}}$	>	$\frac{\sqrt{18}}{\sqrt{13}}$	>	$\frac{\sqrt{40}}{\sqrt{29}}$	>	...

Continuing our proof, we first show that $t \le 5$.

For suppose that $t \ge 6$, then since for every prime π

(8.12) $$\frac{|\pi - 1|}{|\pi|} \le \sqrt{2}$$

we see

(8.13) $$\frac{1}{\sqrt{2}^{t-1}} \prod_{j=1}^{t} \frac{|\pi_j - 1|}{|\pi_j|^{k_j}} \le \frac{1}{\sqrt{2}^{t-1}} \prod_{j=1}^{t} \frac{|\pi_j - 1|}{|\pi_j|} \le \frac{1}{\sqrt{2}^5} \prod_{j=1}^{6} \frac{|\pi_j - 1|}{|\pi_j|}$$

and using lemma (8.11) we find for this

(8.14) $$\le \frac{1}{\sqrt{2}^5} \prod_{j=1}^{6} \frac{|\pi_j - 1|}{|\pi_j|} \le \frac{1}{\sqrt{2}^5} \frac{\sqrt{10}^2}{\sqrt{5}^2} \cdot \frac{4}{3} \cdot \frac{\sqrt{8}^2}{\sqrt{5}^2} \cdot \frac{\sqrt{20}}{\sqrt{13}}$$

which happens to be smaller than

(8.15) $$< 1 - \frac{1}{\sqrt{5}^3 \cdot 3 \cdot \sqrt{13}} \le 1 - \frac{1}{\prod_{j=1}^{t} |\pi_j|^{k_j}} .$$

Combining (8.13), (8.14) and (8.15) we find a contradiction with (8.9) so $t \le 5$.

Next we deal with the cases $t = 1$ and $t = 2$.

If $t = 1$, so $\omega = \pi^k$, then

$$|\omega - 1| = |\pi^k - 1| \ge \sqrt{5}^{k-1} |\pi| - 1$$

which in case $k \ge 2$, exceeds

$$2|\pi| - 1 > |\pi| + 1 \ge |\pi| - 1$$

in contradiction to $\omega - 1 \mid \pi - 1$.

If $t = 2$, so $\omega = \pi_1^{k_1} \pi_2^{k_2}$, we first suppose that $k_1 = k_2 = 1$. Then

(8.16) $\omega - 1 \mid \mathrm{lcm}(\pi_1 - 1, \pi_2 - 1) \Rightarrow \omega - 1$ divides both $\pi_1 - 1$ and $\pi_2 - 1$

because, if π is any prime such that $\pi^k \| \omega - 1$ then $\pi^k \mid \pi_1 - 1$ say, implies $\pi^k \mid ((\omega-1) - \pi_2(\pi_1 - 1)) = \pi_2 - 1$.

Now the righthandside of (8.16) clearly yields a contradiction:

$$|\omega - 1| = |\pi_1 \pi_2 - 1| \ge |\pi_1| \cdot |\pi_2| - 1 \ge \sqrt{5} \cdot |\pi_2| - 1 > |\pi_2| + 1 \ge |\pi_2 - 1|$$

which settles this case. Suppose then that $k_1 \geq 2$, in which case

$$|\omega - 1| = |\pi_1^{k_1}\pi_2^{k_2} - 1| \geq |\pi_1|^{k_1}\cdot|\pi_2| - 1 \geq |\pi_1|^2|\pi_2| - 1$$

together with

$$|\omega - 1| \leq |\mathrm{lcm}(\pi_1 - 1, \pi_2 - 1)| \leq \frac{|\pi_1 - 1|\cdot|\pi_2 - 1|}{|1+i|} \leq \frac{(|\pi_1|+1)(|\pi_2|+1)}{\sqrt{2}}$$

leads to

$$|\pi_2| \leq \frac{|\pi_1| + 1 + \sqrt{2}}{(\sqrt{2}|\pi_1|-1)|\pi_1| - 1} \leq \frac{|\pi_1| + 1 + \sqrt{2}}{2|\pi_1| - 1} \leq \frac{1}{2} + \frac{\frac{3}{2} + \sqrt{2}}{2|\pi_1| - 1} \leq \frac{3}{2}$$

which is impossible for a prime π_2 (not dividing 2).

To deal with the remaining cases $3 \leq t \leq 5$, we first observe the following.

<u>(8.17) Lemma</u>. If $\omega = \prod_{j=1}^{t} \pi_j^{k_j}$ is a pseudoprime, then:

(8.18) $$(\omega - 1) = (\mathrm{lcm}(\pi_j - 1)) = \left((1+i) \prod_{j=1}^{t} \frac{\pi_j - 1}{1+i} \right) .$$

<u>Proof</u>. For every pseudoprime

$$\omega - 1 \mid \mathrm{lcm}(\pi_j - 1) \mid (1+i) \prod_{j=1}^{t} \frac{\pi_j - 1}{1+i} .$$

Suppose that for some prime π also $\pi\cdot(\omega - 1)$ divides the righthand product, then

(8.19) $$|\omega - 1| \leq |\mathrm{lcm}(\pi_j - 1)| \leq \frac{1}{|\pi|} \frac{1}{\sqrt{2}^{t-1}} \prod_{j=1}^{t} |\pi_j - 1| \leq \frac{1}{\sqrt{2}^{t}} \prod_{j=1}^{t} |\pi_j - 1|$$

and so we find using $|\omega| - 1 \leq |\omega - 1|$

(8.20) $$\prod_{j=1}^{t} \frac{|\pi_j - 1|}{|\pi_j|} \geq \prod_{j=1}^{t} \frac{|\pi_j - 1|}{|\pi_j|^{k_j}} \geq \sqrt{2}^{t}\left(1 - \frac{1}{|\omega|}\right)$$

instead of (8.9). Now we use that $t \geq 3$, together with (8.12) and find

(8.21) $$\min_j \frac{|\pi_j - 1|}{|\pi_j|} \geq \sqrt{2}\left(1 - \frac{1}{|\omega|}\right) \geq \sqrt{2}\left(1 - \frac{1}{\sqrt{5}^3}\right) .$$

Using Corollary (8.11) it can easily be seen that this inequality is only satisfied by the prime elements $-2\pm i$ and -3. We see that $\omega = \pi_1^{k_1}\pi_2^{k_2}\pi_3^{k_3}$ with $\pi_1 = -2+i$, $\pi_2 = -2-i$, $\pi_3 = -3$. But now $5 \mid \pi_1\pi_2$ as well as $5 \mid (\pi_1 - 1)(\pi_2 - 1)$; the former implies that $(\omega - 1, 5) = 1$ and the latter that $5 \mid \mathrm{lcm}(\pi_j - 1)$. Like above, with now

$|\pi|$ replaced by 5 , we find that (8.21) can be replaced by

$$\frac{4}{3} = \min \frac{|\pi_j - 1|}{|\pi_j|} \geq 5(1 - \frac{1}{|\omega|}) \geq 5(1 - \frac{1}{15})$$

a contradiction . That proves lemma (8.17) . □

<u>(8.22) Corollary</u>. For a pseudoprime $\omega = \prod_{j=1}^{t} \pi_j^{k_j}$ one has

(8.23) $\forall\, j \neq j' \quad (\pi_j - 1, \pi_{j'} - 1) = (1+i)$, and

(8.24) if one of $-2+i$ and $-2-i$ occurs in the decomposition of ω then no associate of the other does . □

Next we notice that if some $k_{j_0} \geq 2$ in the decomposition of ω , then the condition for pseudoprimality leads to (compare (8.20)):

$$\prod_{j=1}^{t} \frac{|\pi_j - 1|}{|\pi_j|} \geq |\pi_{j_0}| \cdot \prod_{j=1}^{t} \frac{|\pi_j - 1|}{|\pi_j|^{k_j}} \geq |\pi_{j_0}| \sqrt{2}^{t-1} (1 - \frac{1}{|\omega|})$$

so (8.21) is replaced by the even sharper

$$\prod_{j=1}^{t} \frac{|\pi_j - 1|}{|\pi_j|} \geq \sqrt{5}\sqrt{2}^{t-1} (1 - \frac{1}{|\omega|}) \tag{8.25}$$

and therefore proceeding as in the proof of (8.17) leads to the following.

<u>(8.26) Lemma</u>. If $\omega = \prod_{j=1}^{t} \pi_j^{k_j}$ is pseudoprime then $k_1 = k_2 = \ldots = k_t = 1$ □

The cases $t = 4,5$ are easily settled using corollary (8.22), since by (8.23) in the decomposition of a pseudoprime only one of -3 , $-1\pm 2i$, $-3\pm 2i$ may occur ($(1+i)^2$ dividing $\pi - 1$ for each of them), and by (8.24) only one of $-2+i$ and $-2-i$. For $t = 5$, using (8.11),

$$\prod_{j=1}^{5} \frac{|\pi_j - 1|}{|\pi_j|} \leq \frac{\sqrt{10}}{\sqrt{5}} \cdot \frac{4}{3} \cdot \frac{\sqrt{26}^2}{\sqrt{17}^2} \cdot \frac{\sqrt{18}}{\sqrt{13}} \leq \sqrt{2}^4 (1 - \frac{1}{\sqrt{5}^3 \cdot 3 \cdot \sqrt{17}^2})$$
$$\leq \sqrt{2}^4 (1 - \frac{1}{|\omega|})$$

contradicts (8.9) and for $t = 4$ only $\omega = \omega_0 = (-2\pm i)(-3)(-4+i)(-4-i)$ is left as possibility since we find for $\pi | \omega$ with $\frac{|\pi - 1|}{|\pi|}$ minimal by (8.9)

$$\frac{\sqrt{10}}{\sqrt{5}} \cdot \frac{4}{3} \cdot \frac{\sqrt{26}}{\sqrt{17}} \cdot \frac{|\pi - 1|}{|\pi|} \geq \sqrt{2}^3 (1 - \frac{1}{|\omega|}) \tag{8.27}$$

which can by (8.11) easily be seen to imply that this minimal quotient exceeds $\frac{\sqrt{26}}{\sqrt{17}}$. It takes only one norm computation to check that ω_0 is not a pseudoprime, which finishes this case.

So far we proved that a pseudoprime ω is the product of three different prime elements: $\omega = \pi_1\pi_2\pi_3$. Now we treat this final case, by taking

$$\frac{|\pi_1 - 1|}{|\pi_1|} \geq \frac{|\pi_2 - 1|}{|\pi_2|} \geq \frac{|\pi_3 - 1|}{|\pi_3|}$$, using lemma (8.10) and by first trying to satisfy

(8.28) $$\frac{|\pi_1 - 1|}{|\pi_1|} \cdot \frac{|\pi_2 - 1|}{|\pi_2|} \cdot \frac{|\pi_3 - 1|}{|\pi_3|} \geq \sqrt{2}^2\left(1 - \frac{1}{|\pi_1\pi_2\pi_3|}\right) .$$

a) Let $\frac{|\pi_1 - 1|}{|\pi_1|} = \sqrt{2}$, i.e. $\pi_1 = -2\pm i$.

According to (8.24) we have $\pi_2 \neq \bar{\pi}_1$.

(i) Suppose $\frac{|\pi_2 - 1|}{|\pi_2|} = \frac{4}{3}$, i.e. $\pi_2 = -3$.

Using (8.23) to rule out that $(1+i)^2$ divides $\pi_3 - 1$ since it already divides $\pi_2 - 1$,inequality (8.28) leaves the following 17 (pairs of complex conjugated) prime elements π_3 :

$-2\pm3i$, $-2\pm5i$, $-2\pm7i$, $-4\pm i$, $-4\pm5i$, $-6\pm i$, $-6\pm5i$, $-8\pm3i$, $-8\pm5i$, $-8\pm7i$, $-10\pm i$, $-10\pm7i$, $-10\pm9i$, $-12\pm7i$, $-14\pm i$, $-16\pm i$, $-16\pm5i$.

Some computational work leads to the conclusion that out of the 34 remaining possible pairs only one is pseudoprime, namely:

ω or $\bar{\omega} = (-2+i)(-3)(-2-5i)$.

(ii) Let $\frac{|\pi_2 - 1|}{|\pi_2|} = \frac{\sqrt{8}}{\sqrt{5}}$, i.e. $\pi_2 = -1\pm2i$

By (8.24) π_2 is not an associate of $\bar{\pi}_1$.

Using (8.23) we now find 9 pairs of elements satisfying (8.28):

$-2\pm3i$, $-2\pm5i$, $-2\pm7i$, $-4\pm i$, $-4\pm5i$, $-6\pm i$, $-6\pm5i$, $-8\pm3i$, $-10\pm i$.

Only one pseudoprime pair is found:

ω or $\bar{\omega} = (-2+i)(-1-2i)(-2+3i)$

(iii) Suppose $\frac{|\pi_2 - 1|}{|\pi_2|} = \frac{\sqrt{20}}{\sqrt{13}}$, i.e. $\pi_2 = -3\mp2i$ (by (8.24)) .

Here again using (8.22) we see that we have to find π_3 among

$-2\pm3i,\ -4\pm i,\ -6\pm i$.

Of the six possibilities arising, non gives a pseudoprime.

(iv) Suppose $\dfrac{|\pi_2 - 1|}{|\pi_2|} = \dfrac{\sqrt{26}}{\sqrt{17}}$, i.e. $\pi_2 = -4\pm i$.

Now we have to consider

$-2\pm3i,\ -4\mp i,\ -5\pm2i,\ -5\pm4i,\ -6\pm i,\ -7,\ -7\pm2i$,

yielding only one new pair:

ω or $\bar{\omega} = (-2+i)(-4+i)(-2-3i)$.

(v) Suppose $\dfrac{|\pi_2 - 1|}{|\pi_2|} = \dfrac{\sqrt{18}}{\sqrt{13}}$, i.e. $\pi_2 = -2\pm3i$.

Then π_3 is to be found among:

$-2\mp3i,\ -5\pm2i$.

No new pseudoprime is found.

(vi) Finally we find by (8.28) that for $\dfrac{|\pi_2 - 1|}{|\pi_2|} \geq \dfrac{\sqrt{40}}{\sqrt{29}}$:

$$\frac{|\pi_3 - 1|}{|\pi_3|} \geq \frac{\sqrt{29}}{\sqrt{20}}\left(1 - \frac{1}{\sqrt{5}\sqrt{29}|\pi_3|}\right) \geq \frac{\sqrt{40}}{\sqrt{29}} = \frac{|\pi_2 - 1|}{|\pi_2|}$$

for any π_3 with $|\pi_3| \geq \sqrt{13}$, which implies that we will not find any new pseudoprime.

b) Let $\dfrac{|\pi_1 - 1|}{|\pi_1|} = \dfrac{4}{3}$, i.e. $\pi_1 = -3$.

Avoiding extra factors $1+i$, lemma (8.17) and corollary (8.11) show

$$\frac{|\pi_2 - 1|}{|\pi_2|} \leq \frac{\sqrt{26}}{\sqrt{17}} .$$

(i) Suppose that $\dfrac{|\pi_2 - 1|}{|\pi_2|} = \dfrac{\sqrt{26}}{\sqrt{17}}$, i.e. $\pi_2 = -4\pm i$.

We find that we only have to look at

$-4\mp i$, which indeed yields a new pseudoprime , namely:

$\omega = \bar{\omega} = (-3)(-4+i)(-4-i)$.

(ii) For $\dfrac{|\pi_2 - 1|}{|\pi_2|} \lneq \dfrac{\sqrt{26}}{\sqrt{17}}$ an inequality like that in a)(vi) shows that no new pseudoprimes will be found.

c) Let $\dfrac{|\pi_1 - 1|}{|\pi_1|} = \dfrac{\sqrt{8}}{\sqrt{5}}$, i.e. $\pi_1 = -1\pm 2i$.

Now (8.11) and (8.18) imply that

$$\frac{|\pi_2 - 1|}{|\pi_2|} \le \frac{\sqrt{26}}{\sqrt{17}} ,$$

but then by (8.28) we find

$$\frac{|\pi_3 - 1|}{|\pi_3|} \ge \frac{\sqrt{26}}{\sqrt{17}} .$$

This gives only one new possibility, namely: $(-1\pm 2i)(-17)$

which is not a pseudoprime.

d) For $\dfrac{|\pi_1 - 1|}{|\pi_1|} \le \dfrac{\sqrt{20}}{\sqrt{13}}$ we see that $\dfrac{|\pi_2 - 1|}{|\pi_2|} \le \dfrac{\sqrt{26}}{\sqrt{17}}$ and from

(8.28) we then find $\dfrac{|\pi_3 - 1|}{|\pi_3|} \ge 2\dfrac{\sqrt{13}}{\sqrt{20}}\dfrac{\sqrt{17}}{\sqrt{26}}\left(1 - \dfrac{1}{\sqrt{13}\sqrt{17}\sqrt{13}}\right) > \dfrac{\sqrt{26}}{\sqrt{17}}$

contradicting our assumptions.

This ends the case $t = 3$; the seven pseudoprimes found in a)(i),(ii),(iv) and b)(i) are those listed in the statement of the proposition, and therefore the proof of (8.7) is established. □

§9. The $\mathbb{Z}[\rho]$-tests.

In this section we want to use the curves E^{γ} for testing primality in $\mathbb{Z}[\rho]$, analogous to the use of E_{δ} in $\mathbb{Z}[i]$; here E^{γ} is given as before by $Y^2Z = X^3 + \gamma Z^3$.

There is however a slight complication that prevents us from just translating the results of section 7 to this case. For, the proof of theorem (7.7) and its applications were based on the fact that there are only finitely many composite ν satisfying

$$\nu - 1 \mid \operatorname{lcm}(\pi_j - 1) \quad , \quad \pi_j | \nu \ , \quad \pi_j \nmid 2 \ ,$$

which was due to the fact that for every $j \neq j'$ we had $1+i \mid (\pi_j - 1, \pi_{j'} - 1)$.

In $\mathbb{Z}[\rho]$ one does not have the same phenomenon. Therefore there is no reason why there should only be a finite number of small composite solutions to

$$(9.1) \qquad \begin{aligned} &\mu = \prod_{i=1}^{t} \pi_i^{k_i} \quad , \ \pi_i \text{ prime in } \mathbb{Z}[\rho] \ , \quad (\mu,6) = 1 \\ &(\pi_i) \neq (\pi_j) \quad \text{for } i \neq j \\ &\mu - 1 \mid \operatorname{lcm}(\pi_j - 1) \ . \end{aligned}$$

It is not very hard to exhibit an example.

<u>(9.2) Example</u>. Let $\pi_1 = 1+7\rho$, $\pi_2 = -3-7\rho$, $\pi_3 = 16+7\rho$. Then

$$\pi_1\pi_2\pi_3 - 1 = \operatorname*{lcm}_{i\le 3}(\pi_i - 1) = (\pi_1 - 1)(\pi_2 - 1)(\pi_3 - 1) \ .$$

In this case we have $(\pi_i - 1 \, , \pi_j - 1) = 1$ for $i,j \le 3$, $i \neq j$.

One way to overcome this, is by restricting ourselves for the analogon of (7.7) to those curves E^{γ} with the property that (under the proper normalizations) all $\pi_i - 1$ *do* have some non-trivial common factor, namely $1 - \rho$ (the prime above 3), or 2 ; that this can be done and how, is shown in the next proposition.

<u>(9.3) Proposition</u>. Let $\mu \in \mathbb{Z}[\rho]$, $(\mu,6) = 1$.

(i) If $\gamma \in \mathbb{Z}[\rho]$ with $(6\mu,\gamma) = 1$ satisfies

(9.4) $\gamma \equiv \beta^3 \bmod \mu$ for some β

then for every prime π dividing μ, with $\pi \equiv \overline{\left(\frac{\gamma}{\pi}\right)_6} \bmod 2(1-\rho)$

we have: $2 \mid \pi - 1$.

(ii) If $\gamma \in \mathbb{Z}[\rho]$ with $(6\mu,\gamma) = 1$ satisfies

(9.5) $\gamma \equiv \beta^2 \bmod \mu$ for some β

then for every prime π dividing μ, with $\pi \equiv \overline{\left(\frac{\gamma}{\pi}\right)_6} \bmod 2(1-\rho)$

we have: $1-\rho \mid \pi - 1$.

Proof. If $\gamma \equiv \beta^3 \bmod \mu$ then for every prime $\pi|\mu$ we have $\left(\frac{\gamma}{\pi}\right)_3 = \left(\frac{\beta^3}{\pi}\right)_3 = 1$ and thus we find $\overline{\left(\frac{\gamma}{\pi}\right)_6} = \pm 1$. Then $\pi \equiv \pm 1 \bmod 2(1-\rho)$ so $\pi \equiv 1 \bmod 2$. The other case is proved similarly.

(9.6) Remarks. Conditions (9.4) and (9.5) also have a geometric meaning: it provides E^γ with certain torsion. Indeed, γ being a cube in $\mathbb{Z}[\rho]/(\mu)$ means that E^γ has 2-torsion modulo μ , since in this case the point $(-\beta : 0 : 1)$ on $Y^2Z = X^3 + \beta^3 Z^3$ is its own inverse, while γ equal to a square gives $(1-\rho)$-torsion on E^γ , since then the point $(0 : \beta : 1)$ is on $Y^2Z = X^3 + \beta^2 Z^3$ and satisfies:

$$\rho\cdot(0 : \beta : 1) = (\rho\cdot 0 : \beta : 1) = (0 : \beta : 1) .$$

For *prime* μ we see that these are equivalent:

$$\gamma \equiv \beta^3 \bmod \mu \quad \text{for some } \beta \iff E^\gamma \quad \text{has 2-torsion,}$$

$$\gamma \equiv \beta^2 \bmod \mu \quad \text{for some } \beta \iff E^\gamma \quad \text{has } (1-\rho)\text{-torsion} .$$

Next we show that pseudoprimes in $\mathbb{Z}[\rho]$ do not exist if we insist that all $\pi - 1$ have a factor 2 or $1-\rho$ in common.

(9.7) Proposition. Let $\mu = \prod_{i=1}^{t} \pi_i^{k_i}$ in $\mathbb{Z}[\rho]$, $\pi_i \neq \pi_j$ for $i \neq j$ all prime and $(\mu,6) = 1$. If {or all i : $2 | \pi_i - 1$ or for all i : $1-\rho \mid \pi_i - 1$ then $\mu - 1 \mid \operatorname{lcm}(\pi_i - 1) \Rightarrow t = 1 = k_1$: μ is prime .

Proof. In case $1-\rho$ divides all $\pi_i - 1$ then the following inequality yields for all $t > 2$ a contradiction with the required divisibility:

(9.8) $$\frac{1}{|\mu|}\left|(1-\rho)\prod_{i=1}^{t}\frac{\pi_i-1}{1-\rho}\right| \le \frac{1}{\sqrt{3}^{t-1}}\prod_{i=1}^{t}\frac{|\pi_i-1|}{|\pi_i|} \le \frac{1}{\sqrt{3}^{t-1}}\prod_{i=1}^{t}\frac{(\sqrt{7}+1)}{\sqrt{7}} <$$

$$< (1-\frac{1}{\sqrt{7}^t}) \le 1-\frac{1}{|\mu|}$$

using that $|\pi_i| > \sqrt{7}$; for $t=2$ we may proceed just the same as in the previous section . Inequality (9.8) applies with $\sqrt{3}$ replaced by 2 directly for all $t>1$ in case 2 divides all $\pi_i - 1$. This leaves only the case $t=1$ and $k>1$ to deal with, which under either of the assumptions is settled by:

$$\frac{|\pi-1|}{|\mu|} \le \frac{1}{\sqrt{7}^{k-1}}\frac{|\pi-1|}{|\pi|} \le \frac{1}{\sqrt{7}}\left(\frac{\sqrt{7}+1}{\sqrt{7}}\right) < (1-\frac{1}{\sqrt{7}}) \le 1-\frac{1}{|\mu|}$$

which again contradicts divisibility of the lcm by $\mu - 1$.

This proves (9.7). □

We now give the results analogous to those of section 7.

<u>(9.9) Theorem</u>. Let $\mu \in \mathbb{Z}[\rho]$ and let $\sigma \in \mathbb{Z}[\rho]$ divide $\mu - 1$.
If there exist $\gamma \in \mathbb{Z}[\rho]$ with $(6\gamma,\mu) = 1$ and points P_i on $E\ (\mathbb{Z}[\rho]/(\mu))$ satisfying:

(9.10) for all i : $(\mu-1)\cdot P_i = 0_{E^\gamma}$

and

(9.11) for every $\pi|\sigma$, $\pi \in \mathbb{Z}[\rho]$ prime, there exists a i such that for every non-unit $\tau \in \mathbb{Z}[\rho]$, $\tau|\mu$ we have $(\frac{\mu-1}{\pi})\cdot P_i \not\equiv 0_{E^\gamma} \bmod \tau$

then every divisor ω of μ , normalized by

$$\omega \equiv \overline{\left(\frac{\gamma}{\omega}\right)_6} \bmod 2(1-\rho)$$, satisfies

(9.12) $\omega \equiv 1 \bmod \sigma$.

If moreover $\sigma \nmid 6$ then also

$$\mu \equiv \overline{\left(\frac{\gamma}{\mu}\right)_6} \bmod 2(1-\rho) .$$ □

<u>(9.13) Corollary</u>. $(|\sigma| - 1)^2 > |\mu| \Rightarrow \mu$ prime in the above.□

(9.14) Theorem. Let $\mu \in \mathbb{Z}[\rho]$.

If there exist $\gamma \in \mathbb{Z}[\rho]$ with

(9.15) $(6\gamma, \mu) = 1$ and

(9.16) either $\gamma \equiv \beta^3$ or $\gamma \equiv \beta^2 \mod \mu$ for some $\beta \in \mathbb{Z}[\rho]$,

and points P_i on $E^{\gamma}(\mathbb{Z}[\rho]/(\mu))$ satisfying

(9.17) $\forall i : (\mu - 1) \cdot P_i = 0_{E^{\gamma}}$

(9.18) $\forall$ prime $\pi | \mu - 1 \quad \exists i : (\frac{\mu - 1}{\pi}) \cdot P_i \neq 0_{E^{\gamma}}$

then μ is prime in $\mathbb{Z}[\rho]$.

(9.19) Remarks. Of course the remarks made in section 7 carry over; we emphasize here again that for (9.9) all factors found for all associates of μ minus 1 can be used : so here we use even the factored part of $\mu^6 - 1$.

REFERENCES

[A-McD] : M.F. Atiyah and I.G. MacDonald, Introduction to commutative algebra, Addison-Wesley, Reading 1969.

[BLSTW] : John Brillhart, D.H. Lehmer, J.L. Selfridge, Bryant Tuckerman, and S.S. Wagstaff, Jr, Factorizations of $b^n \pm 1$, Contemporary mathematics *22*, Am. Math. Soc. 1983.

[CASS] : J.W.S. Cassels, Diophantine equations with special reference to elliptic curves, J. London Math. Soc. *41* (1966), 193-291.

[DEUR] : Max Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hamburg *14* (1941), 197-272.

[FULT] : William Fulton, Algebraic curves, Benjamin, New York, 1969.

[HA-DA] : H. Davenport and H. Hasse, Die Nullstellen der Kongruenz-zetafunktionen in gewissen zyklischen Fällen, J. Reine und Angew. Math. *172* (1935), 151-182.

[HART] : Robin Hartshorne, Algebraic geometry, GTM 52, Springer, New York etc. 1977.

[IR-RO] : Kenneth Ireland and Michael Rosen, A classical introduction to modern number theory, GTM 84, Springer, New York etc. 1982.

[LANG]1 : Serge Lang, Elliptic curves, diophantine analysis, Springer Berlin etc. 1978.

[LANG]2 : Serge Lang, Algebra, Addison-Wesley, Reading 1980.

[LA-RU] : H. Lange and W. Ruppert, Complete systems of addition laws on abelian varieties, Invent. Math. *79* (1985), 603-610.

[LEHM] : D.H. Lehmer, Strong Carmichael numbers, J. Austral. Math. Soc. Ser. A, *21* (1976), 508-510.

[LENS] : H.W. Lenstra, Jr, Divisors in residue classes, Dep. of Math. Report 83-03, University of Amsterdam 1983.

[ROBE] : Alain Robert, Elliptic curves, Lecture Notes 326, Springer, Berlin etc. 1973.

[SCHO] : René Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp. *45* (1985)

[SHAF] : I.R. Shafarevic, Basic algebraic geometry, Springer, Berlin etc. 1977.

[SH-TA] : G. Shimura and Y. Taniyama, Complex multiplication of abelian varieties (and its applications to number theory), Math. Soc. of Japan, 1961.

[SO-ST] : R. Solovay and V. Strassen, A fast Monte-Carlo test for primality, SIAM J. Comput. *6* (1977), 84-85; err. *7* (1978), 118.

[TATE] : John.T. Tate, The arithmetic of elliptic curves, Invent. Math. *23* (1974), 179-206.

[WILL] : H.C. Williams, Primality testing on a computer, Ars Combin. *5* (1978), 127-185.