III-1. [Miller-Rabin]

The Miller-Rabin test is an efficient *probabilistic compositeness* test: the input is an odd integer $n > 2$ and the output is either a witness to the compositeness of n or the claim that n is 'probably prime'; in the latter case there is also an upper bound on the 'probability' that n is composite after all. This test is typically employed before starting a factorization algorithm (like Pollard-ρ).

The simple test uses two facts for prime numbers n, namely Fermat's little theorem (stating that always $a^n \equiv a \bmod n$) and the fact that $x^2 \equiv 1 \bmod n$ only has solutions $\pm 1 \bmod n$. It proceeds as follows: find odd d and integer $k \geq 1$ such that $n - 1 = 2^k \cdot d$. Then choose a with $1 < a < n - 1$ random and compute successively

$b_0 \equiv a^d \bmod n$;
$b_1 \equiv b_0^2 \bmod n$,
$b_2 \equiv b_1^2 \bmod n$, and so on:
$b_j \equiv b_{j-1}^2 \bmod n$

but stop as soon as one of the following cases occurs:

(A) $b_j \equiv 1 \bmod n$;
(B) $j = k$;
(C) $b_j \equiv -1 \bmod n$.

When ending in (A) with $j > 0$, or in (B), declare n to be composite. When ending in (C) (with $j < k$) or in (A) with $j = 0$, declare n possibly prime; in this case, repeat the test with a new random choice for a, and declare n *probably prime with probability of error less than* 4^{-t} if this case occurs for each of t (say 20) choices for a. It can be shown that for $n > 9$ composite at least $3/4$ of the possible choices for a leads to the correct declaration of n being composite.

(i) Implement this test.
(ii) Prove that the test will never declare prime numbers to be composite.
(iii) Find some composite numbers that satisfy $a^{n-1} \equiv 1 \bmod n$ for all a coprime to n; conclude that such number would most likely fail a weaker probabilistic test that declares n composite if random a is found with $a^{n-1} \not\equiv 1 \bmod n$.
(d) Prove the probabilty statement (with the weaker error bound 2^{-t}).

III-2. [Pell]

(i) Implement an algorithm that on input an element $\alpha \in \mathbf{Q}(\sqrt{d})$ (for some positive squarefree integer $d > 1$) returns the continued fraction expansion of α as output, in the form of a pair of sequences containing pre-period and period of the expansion.
(ii) Use your algorithm to find some values for d with long continued fraction period (compared to $\sqrt{(d)}$). item(iii) Also write a function that returns, for given d, both the sign $\epsilon \in \{-1, 1\}$ and the smallest solution (x, y) for the equation $x^2 - dy^2 = \epsilon$.

III-3. [Common continued fractions]
Implement the 'common continued fraction' algorithm (see attached description) that is of (almost) linear rather than (almost) quadratic complexity.

IV-1.

(i) When we denote the units of a ring S by S^*, prove that under the conditions for the Chinese Remainder Theorem:

$$(R/m)^* = (R/m_1)^* \times \cdots (R/m_k)^*.$$

(ii) For an integer $m > 1$ we define the Euler-ϕ function as $\phi(m) = \#(\mathbf{Z}/m\mathbf{Z})^*$. Prove that if m is an integer with prime factorization $m = p_1^{e_1} \cdots p_k^{e_k}$ (distinct primes p_i and positive exponents e_i:

$$\phi(m) = m \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).$$

(iii) Find all m with $\phi(m) < 25$.

(iv) For polynomials f over a finite field $\mathbf{F}_q$ of degree n we define $\Phi(f) = \#\mathbf{F}_q[x]/(f)^*$, so the number of polynomials over $\mathbf{F}_q$ of degree less than n coprime to f. Show that $\Phi(f) = q^n - 1$ if f is irreducible, that $\Phi(f) = (q^d - 1)q^{n-d}$ if f is a power of an irreducible polynomial of degree d and that

$$\Phi(f) = q^n \cdot (1 - \frac{1}{q^{n_1}}) \cdot (1 - \frac{1}{q^{n_2}}) \cdots (1 - \frac{1}{q^{n_k}}),$$

if $f = f_1^{e_1} \cdots f_k^{e_k}$ is a factorization in irreducible polynomials f_i of degree n_i.

IV-2. [mixed radix]
Implement Garner's algorithm for the Chinese Remainder Algorithm. Check it against Example 5.15 from Geddes et al.