Eindopdracht: Probabilistische Primaliteit

Het doel van deze opdracht is om met Magma een efficiënte test te maken waarmee kan worden *bewezen* dat een getal *samengesteld* (niet priem) is, of *aannemelijk gemaakt* kan worden dat het priem is. Daarover moet je ook een kort verslag in LaTeX schrijven.

De test

Deze test maakt gebruik van twee belangrijke eigenschappen van priemgetallen: als n priem is, dan is $a^{n-1} \equiv 1 \bmod n$, en dan heeft de vergelijking $x^2 \equiv 1 \bmod n$ alleen de oplossingen $x \equiv \pm 1 \bmod n$.

De test verloopt als volgt: vind een oneven d en een gehele $k \geq 1$ zodat $n - 1 = 2^k \cdot d$ (vanaf nu is n groter dan 2 en oneven). Kies een willekeurig getal a tussen 1 en n en bereken achtereenvolgens $b_0 \equiv a^d \bmod n$; $b_1 \equiv b_0^2 \bmod n$, $b_2 \equiv b_1^2 \bmod n$, ... , $b_j \equiv b_{j-1}^2 \bmod n$ maar stop zodra één van de volgende gevallen optreedt (test ze in deze volgorde!):

(A) $b_j \equiv 1 \bmod n$;

(B) $j = k$;

(C) $b_j \equiv -1 \bmod n$.

Als je in (B) eindigt (en dus $b_k \not\equiv 1 \bmod n$) dan weet je zeker dat n samengesteld is; dat is ook het geval wanneer je eindigt in geval (A) met $j > 0$. Alleen wanneer je in geval (C) eindigt (met een $j < k$) of in geval (A) met $j = 0$ dan is het mogelijk dat n een priemgetal is. In dat geval kun je de test herhalen met een andere keuze voor a.

Wanneer n geen kwadraat, derdemacht, enz. is, maar wel samengesteld, geeft minstens een kwart van de verschillende mogelijkheden voor a via deze test daarvoor een bewijs; dan is de kans dus heel klein (”kleiner dan 1 op de miljoen”) dat je bij 20 willekeurige keuzes van a met deze test zo'n bewijs niet vindt. We verklaren n daarom *waarschijnlijk priem* als we na 20 tests geen bewijs hebben gevonden dat n samengesteld is.

De opdrachten

(1) Schrijf een functie die van een positief geheel getal n snel nagaat of $n = m^e$ voor een $e > 1$ (en een natuurlijk getal m). [Hint: `Log`, `Round`, `Root`]

(2) Schrijf een functie in Magma die bij gegeven oneven $n > 2$ de getallen k en d vindt met d oneven en $2^k \cdot d = n - 1$. [Hint: `div`]

(3) Schrijf een functie die voor positieve gehele getallen a, d, n efficiënt uitrekent wat $a^d \bmod n$ is. [Hints: om a^d snel uit te rekenen moet je niet herhaald vermenigvuldigen met a, maar kwadrateren en vermenigvuldigen, bijvoorbeeld door $a, a^2, a^4, a^8, \ldots$ uit te rekenen, en dan de machten die je nodig hebt met elkaar vermenigvuldigen. Om efficiënt modulo n te rekenen moet je na elke vermenigvuldiging het resultaat weer modulo n nemen. Gebruik bijvoorbeeld `Intseq(d, 2)`, `mod`.]

(4) Schrijf een functie die bij gegeven oneven $n > 2$ en $1 < a < n$ de rij $b_0, b_1, b_2, \ldots$ (niet verder dan nodig) uitrekent om te bepalen of je eindigt in geval (A), (B), of (C).

(5) Schrijf een functie die bij gegeven oneven $n > 2$ de voorgaande functies aanroept op 20 willekeurig gekozen waarden van a, en als resultaat afdrukt `"n is samengesteld"` of `"n is waarschijnlijk priem"`. [Hint: `Random`, `print`, controleren met `IsPrime`.]

Het verslag

Wanneer de programmeeropdracht is voltooid leg je je bevindingen in een paar bladzijden LaTeX uit; in het bijzonder leg je uit waarom de conclusies van de test kloppen.

Inleveren

Magma-programma en LaTeX-bestand vóór 1 maart 2007 per e-mail inleveren bij Wieb Bosma: `bosma@math.ru.nl`.