Een 'amusante' ontbinding

Beschouw het getal

$$14989086475$$

Splits de cijfers in twee groepjes

$$14989086475$$

Neem som en verschil van de twee delen:

$$149890 + 86475 = 236365$$

$$149890 - 86475 = 63415$$

Vermenigvuldig ze

$$236365 \times 63415 = 14989086475.$$

Ontbinding op de computer

Pari opgave

De PARI opdracht `factor(n)` stelt ons in staat om getallen n tot ongeveer 80 cijfers te ontbinden.

- Probeer `factor(2^n-1)` voor een aantal priemgetallen n. Als je geen priemgetallen kunt bedenken gebruik dan `prime(k)`, het k-de priemgetal.
- Kies een random getal `n=random(10^50)` en ontbind n. Herhaal dit een aantal malen.

Een niet zo naïeve ontbindingsmethode

Gegeven N, ontbind N in priemfactoren.

Algemeen idee: Vind x, y zó dat $x^2 - y^2 = (x - y)(x + y)$ deelbaar is door N. Bereken vervolgens $\mathrm{ggd}(N, x - y)$ en $\mathrm{ggd}(N, x + y)$.

Met enig geluk is één van deze getallen een deler van N.

Het ggd van twee getallen kan in polynomiale tijd worden berekend met het Euclidisch algoritme. Bijvoorbeeld $\mathrm{ggd}(2913, 1533)$.

- $2913 - 1533 = 1380$
- $1533 - 1380 = 153$
- $1380 - 9 \times 153 = 3$
- $153 - 51 \times 3 = 0$

De laatste rest $\neq 0$ is de gewenste ggd. Dus $\mathrm{ggd}(2913, 1533) = 3$.

Kwadratische zeef

Stel $r = \lfloor \sqrt{N} \rfloor + 1$ en kies een grens B. Bereken $(k+r)^2 - N$ voor kleine k en selecteer de getallen waarvan alle priemdelers $\leq B$ zijn.
Voorbeeld: $N = 123889$. Dan $r = \lfloor \sqrt{N} \rfloor + 1 = 352$. Kies $B = 13$ en probeer $-20 \leq k \leq 20$.
We vinden de volgende waarden van k waarvan $(r+k)^2 - N$ uit priemfactoren ≤ 13 bestaat,

k	$(r+k)^2 - N$
-19	$-2^3 \cdot 5^3 \cdot 13$
-17	$-2^4 \cdot 3^6$
-9	$-2^5 \cdot 3 \cdot 5 \cdot 13$
0	$3 \cdot 5$
1	$2^4 \cdot 3^2 \cdot 5$
7	$2^7 \cdot 3 \cdot 13$
15	$2^4 \cdot 3^3 \cdot 13$

Finish

Kies de verschillen met $k = -19, -9, 15$,

$$\begin{aligned}(r-19)^2 &\equiv -2^3 \cdot 5^3 \cdot 13 (\mathrm{mod}\ N)\\ (r-9)^2 &\equiv -2^5 \cdot 3 \cdot 5 \cdot 13 (\mathrm{mod}\ N)\\ (r+15)^2 &\equiv 2^4 \cdot 3^3 \cdot 5^2 (\mathrm{mod}\ N)\end{aligned}$$

Vermenigvuldiging van deze congruenties geeft

$$(r-19)^2(r-9)^2(r+15)^2 \equiv (2^6 \cdot 3^2 \cdot 5^3 \cdot 13)^2 (\mathrm{mod}\ N)$$

We hebben twee verschillende kwadraten, gelijk modulo N. Kijk of dit een factor van N geeft,

$$\begin{aligned}& \mathrm{ggd}(N, (r-19)(r-9)(r+15) - 2^6 \cdot 3^2 \cdot 5^3 \cdot 13)\\ = \ & \mathrm{ggd}(123889, 40982373) = 541\end{aligned}$$

We hebben geluk en vinden $N = 541 \cdot 229$.

Lineaire algebra

De exponent vectoren van onze ontbindingen modulo 2,

k	-1	2	3	5	7	11	13
-19	1	1	0	1	0	0	1
-17	1	0	0	0	0	0	0
-9	1	1	1	1	0	0	1
0	0	0	1	1	0	0	0
1	0	0	0	1	0	0	0
7	0	1	1	0	0	0	1
15	0	0	1	0	0	0	0

De som van de rijen bij $k = -19, -9, 15$ is nul modulo 2.
Uit lineaire algebra volgt dat als het aantal rijen groter is dan het aantal kolommen dan is er zeker een oplossing.

Looptijd

Heuristische looptijd:

$$L(N) = \exp\left(2\sqrt{\log(N)\log\log(N)}\right).$$

Oefening:

$$\lim_{N\to\infty} L(N)/N^{\epsilon} = 0$$

voor elke $\epsilon > 0$.
De kwadratische zeef is een *subexponentieel algoritme*.

Cryptografie en priemontbinding

Kies verschillende priemgetallen p, q van 100 tot 200 cijfers.
Bereken $N = pq$.

Lemma

Stel $M = k(p-1)(q-1)+1$ met k willekeurig geheel. Dan geldt $a^M \equiv a \pmod{N}$ voor alle gehele getallen a.

Bewijs: We berekenen eerst $a^M \pmod{p}$.

1. Stel dat p niet a deelt. Pas Fermat toe: $a^M \equiv a^{k(p-1)(q-1)+1} \equiv 1 \cdot a \equiv a \pmod{p}$.
2. Als a deelbaar is door p dan geldt $a^M \equiv 0 \equiv a \pmod{p}$.
3. Conclusie $a^M \equiv a \pmod{p}$ voor alle a. Op dezelfde manier $a^M \equiv a \pmod{q}$ voor alle a.
4. Dus $a^M - a$ wordt gedeeld door zowel p als q en daarmee door $pq = N$.

RSA-cryptografie

We beschrijven het RSA-protocol, genoemd naar Rivest-Shamir-Adleman (1977), om berichten te versleutelen en ontsleutelen.
De ingredienten zijn de eerder genoemde p, q van 100 tot 200 cijfers en hun product N.
Kies een willekeurig getal E, je publieke sleutel, en bepaal het getal F, je geheime sleutel, zó dat $EF = k(p-1)(q-1)+1$ voor zekere k.
Stel iemand wil je een bericht sturen, gepresenteerd door een getal B. Uit voorgaand lemma weten we dat $B^{EF} \equiv B (\mathrm{mod}\ N)$.
In plaats van B kan de verzender het versleutelde bericht $C = B^E (\mathrm{mod}\ N)$ naar je versturen. Bij ontvangst bereken je $C^F \equiv (B^E)^F \equiv B^{EF} \equiv B (\mathrm{mod}\ N)$.

NB: Als je F uit E wilt afleiden heb je p, q nodig en dus de ontbinding van N.

RSA in PARI

De stappen uit de vorige slide kun je in PARI uitvoeren:

- `p=randomprime(10^50)` en `q=randomprime(10^50)`
- `n=p*q`
- `e=137` (publieke sleutel, zelf te kiezen oneven getal)
- `f=lift(1/Mod(e,(p-1)*(q-1)) )` (geheime sleutel. Dit kan misgaan, kies dan een andere e)
- `b=123456789` (Kies zelf een bericht)
- `c=Mod(b,n)^e` (versleutel het)
- `c^f` (ontsleuteling)
- `lift(c^f)` (ontsleuteling zonder dat n geprint wordt)

Dit kan levensecht worden gemaakt met twee personen. Eén persoon maakt n en de sleutels e, f aan en stuurt n en e naar persoon twee. Deze verzint een bericht b en stuurt $b^e \pmod{n}$ naar persoon één. Deze ontsleutelt het bericht.