Day 25 4/15/98 "You have to squint a little."

1 Primality Testing

Is n prime or composite? We want an algorithm that runs in $(\log n)^k$.

1.1 Fermat's little theorem

If p is prime with $1 < a < p$ then $a^{p-1} = 1 \bmod p$

1.2 contrapositive

If $1 < a < n$ and $a^{n-1} \neq 1 \bmod n$ then n is composite.

1.3 Primality test heuristic

1. guess a
2. check if $a^{n-1} \neq 1 \bmod n$ If yes output 'composite' otherwise output 'possibly prime'

This heuristic fails for certain numbers known as Carmicheal numbers. Example:

$561 = 3 * 11 * 17$
If $GCD(a, n) = 1$ then $a^{n-1} = 1 \bmod n$
n is Carmicheal if

1. n is composite
2. $\lambda(n)$ divides $n - 1$ with $n = p_1^{\alpha_1}...p_m^{\alpha_m}$ and $\lambda(n) = LCM(p_1^{\alpha_1 - 1}(p_1 - 1), ..., p_m^{\alpha_m - 1}(p_m - 1))$

Carmicheal numbers actually always have $\alpha_i = 1$ and $m \geq 3$.

1.4 More number theory (from gauss)

± 1 are the only roots of $x^2 = 1 \bmod p$ with p prime

1.5 Better algorithm

A(a, n)
let $n - 1 = 2^t u$ for u odd

1. if $n = 2$ output 'prime'
2. if n is even, output 'composite'
3. if $a^u = 1 \bmod n$ output 'possibly prime'
4. if $a^{2^j u} = -1 \bmod n$ for $1 \leq j < t$ output 'possibly prime'
5. else, output 'composite'

1.6 Theorem

half the $a \in [1, n]$ for n composite will have that $A(a, n)$ return 'composite'.

This means that if you run $A(a, n)$ 100 times each time putting out 'possibly prime' then either n is prime or you are very unlucky.

1.7 Some number theory

- Z_n = the ring with $+, *\text{mod}n = \{0, 1, ..., n-1\}$
- $|Z_n| = n$
- R, R' = rings then $R \times R' = \{(r, r')|r \in R, r' \in R'\}$ is a ring with $(r_1, r_1^{'}) + (r_2, r_2^{'}) = (r_1 + r_2, r_1^{'} + r_2^{'})$.

1.7.1 Chinese remainder theorem

For $n = p_1^{\alpha_1} * ... * p_m^{\alpha_m}$

we have: $Z_n \simeq Z_{p_1^{\alpha_1}} \times Z_{p_m^{\alpha_m}}$

For $a \in Z_n$ $a \rightarrow (a\text{mod}p_1^{\alpha_1}, ..., a\text{mod}p_m^{\alpha_m})$

1.7.2 multiplicative group

$Z_n^* = \{a \in Z_n | \exists a' \text{with } a' * a = 1\text{mod}n\} = \{a \in Z_n | GCD(a, n) = 1\}$

If p is an odd prime, then Z_p^* is a cyclic group, which means every invertible element can be found by multiplying some base (a 'generator') mod$p$.

1.8 Pulling all the facts together

if $n = 5 * 7$ then $Z_{35}^* \simeq Z_5^* \times Z_7^* \simeq C_4 * C_6$ then there will be many solutions to $x^2 = 1\text{mod}35$.

For 35, $x = 1, 6, -6, 34$ will work.

Working in the decomposed group, we get:

1. $1 \rightarrow (1, 1)$
2. $6 \rightarrow (1, -1)$
3. $-6 \rightarrow (-1, 1)$
4. $34 \rightarrow (-1, -1)$

$6^2 = 1\text{mod}35$ = a 'nontrivial square root of 1' => 35 is composite.