Prime numbers

A natural number $p \neq 1$ is prime if and only if it has no factors (divisors) other than 1 and itself.

Fundamental Theorem of Arithmetics.

Any positive integer n can be expressed as the product of powers of primes in a way that is unique up to a possible reordering of factors.

Thm (Euclid 300 BC) There are infinitely many prime numbers.

proof: Assume that there are exactly N primes, $p_1 = 2, p_2 = 3, \ldots p_N$

Then $m = (p_1 \cdot p_2 \cdots p_N) + 1$ is an integer bigger than $p_1, p_2, \ldots p_N$ which is not divisible by any of the primes $p_1, p_2, \ldots p_N$, contradiction.

Thm (Prime Number Theorem) Let $\pi(x)$ be the number of primes less than or equal to x. Then $\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1$

Fermat's little Theorem

Let p be a prime number.

a) if a is relatively prime to p, then $a^{p-1} \equiv 1 \pmod{p}$.

b) $a^p \equiv a \pmod{p}$ for any integer a

proof a) Let $a \in \{1, 2, \ldots p-1\}$. Consider the numbers

$$a \cdot 1 \bmod p \quad a \cdot 2 \bmod p \quad \ldots \quad a \cdot (p-1) \bmod p$$

These are all distinct, and in the range $1, 2, \ldots p-1$. Otherwise, suppose by contradiction, that $a \cdot i \bmod p = a \cdot j \bmod p$ for some $1 \leq i < j \leq p-1$

Then $a(i-j) \equiv 0 \pmod{p} \Rightarrow a(i-j)$ is divisible by p. However this is impossible because p is prime, and $p \nmid a$ and $p \nmid i-j$.

In conclusion, multiplying by a has rearranged the numbers $1, 2, \ldots p-1$.

$$(a\cdot 1)\cdot(a\cdot 2)\cdots(a\cdot(p-1)) \equiv 1\cdot 2\cdots p-1 \pmod p.$$

$$a^{p-1}\cdot(1\cdot 2\cdots(p-1)) \equiv (1\cdot 2\cdots(p-1)) \pmod p.$$

$\Rightarrow$ $a^{p-1}\equiv 1 \pmod p$ because $1\cdot 2\cdots(p-1)$ is relatively prime to p. hence invertible mod p.

Theorem (Euler) Let p and q be distinct primes.

a) if a is relatively prime to p and to q, then $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$

b) if a is any integer, and k is any positive integer, then

$$a^{k(p-1)(q-1)+1} \equiv a \pmod{pq}.$$

proof: a)

a is relatively prime to p and p is prime, so by Fermat's theorem we have

$$a^{p-1} \equiv 1 \pmod p.$$

a is relatively prime to q (which is prime) so by Fermat's Thm we know that

$$a^{q-1} \equiv 1 \pmod q.$$

Then we have:

$$\left(a^{p-1}\right)^{q-1} \equiv 1 \pmod p \Rightarrow \left(a^{p-1}\right)^{q-1} - 1 \equiv 0 \pmod p.$$

$$\left(a^{q-1}\right)^{p-1} \equiv 1 \pmod q \Rightarrow \left(a^{q-1}\right)^{p-1} - 1 \equiv 0 \pmod q$$

$\Rightarrow$

$p \mid \left(a^{p-1}\right)^{q-1} - 1$

$q \mid \left(a^{q-1}\right)^{p-1} - 1$

Since p and q are distinct primes

$\Rightarrow$ $pq \mid a^{(p-1)(q-1)} - 1$

$\Leftrightarrow$ $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$

Example: Compute $3^{12} \pmod{26}$

$$3^{(13-1)(2-1)} \equiv 1 \pmod{26}.$$

Thm. Fermat Let p be a prime number.

1. If a is relatively prime to p, then $a^{p-1} \equiv 1 \pmod{p}$.
2. If a is any integer, then $a^p \equiv a \pmod{p}$

Thm Euler Let p and q be distinct prime numbers

1. If a is relatively prime to p, then $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$
2. If a is any integer, and k is any positive integer, then
$$a^{k(p-1)(q-1)+1} \equiv a \pmod{pq}$$

Observation important for Cryptography

whenever two positive integers d and e satisfy $d \cdot e = 1 + k(p-1)(q-1)$
or equivalently $d \cdot e \equiv 1 \mod ((p-1)(q-1))$

then the functions

$E(x) = x^e$ MOD pq $\quad 1 \le x \le pq-1$ and

$D(y) = y^d$ MOD pq $\quad 1 \le y \le pq-1$ are inverses

$$E(D(y)) = E(y^d) = (y^d)^e = y^{de} = y^{1+k(p-1)(q-1)} = y \pmod{pq}$$
$$D(E(x)) = D(x^e) = (x^e)^d = x^{de} = x^{1+k(p-1)(q-1)} = x \pmod{pq}.$$

$$x \xrightarrow{E} y = x^e \text{ MOD } pq \xrightarrow{D}$$

RSA public key cryptosystem

100-200 decimal digits

Alice – selects two distinct primes p and q.
– computes $m = pq$, $n = (p-1)(q-1)$.
– selects a number e which is relatively prime to n
– and uses the Extended Euclidean Algorithm to find the multiplicative inverse of e mod n, that is an integer d such that $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$

Alice broadcasts e and m.
m is called the modulus
e is the public key or encryption key

Alice keeps d and p and q a secret
d is the private key or decryption key

Bob – has a message to send to Alice

message = number x in range $0, m-1$.

– uses Alice's pubic key e and modulus m to encrypt the message:

$$y = x^e \text{ MOD } m$$

– sends y to Alice.

Alice – receives y from Bob

– uses her private key d to decode the message:

$$x = y^d \text{ MOD } m$$

$$y^d \equiv (x^e)^d \equiv x^{ed} \pmod m \equiv x \pmod m$$ because

$ed \equiv 1 \bmod ((p-1)(q-1)) \Rightarrow ed = 1 + k(p-1)(q-1)$

By Euler's theorem $x^{1+k(p-1)(q-1)} \equiv x \pmod m$

Bob – performs the same setup as Alice

choose two distinct primes p and q, etc ...

Cryptanalysis – essentially equivalent to factoring m

– the factors are large ~ 200 digits.

– the security of the RSA resides in the hardness/time consuming problem of factoring

Example :

+ select primes $p = 11$ and $q = 3$

- compute $m = pq = 33$ and $n = (p-1)(q-1) = (11-1)(3-1) = 20$

- choose e relatively prime with $n = 20$

$e = 3$

- find d such that $e \cdot d \equiv 1 \pmod{20}$

$d = 7$

Euclidean Alg: find s, t such that $3s + 20t = 1$.

$20 = 6 \cdot 3 + 2 \Rightarrow 0 = -2 - 3 \cdot 6 + 20$ $\mapsto$ $1 = 7 \cdot 3 - 20$

$3 = 2 + 1 \Rightarrow 1 = -2 + 3$ $\Rightarrow$ $3^{-1} \equiv 7 \pmod{20}$

$GCD(20, 3) = GCD(3, 2) = GCD(2, 1) = 1$

- public key $(e, m) = (3, 33)$

- private key $(d, m) = (7, 33)$

Bob wants to encrypt the message $x = 14$, using Alice's public key

$y = x^e \pmod{m}$

$y = 14^3 \pmod{33} = 2744 \pmod{33} = 83 \cdot 33 + 5 \pmod{33}$

$2744 = 83 \cdot 33 + 5$

Hence the ciphertext is $y = \boxed{5}$

Alice - receives the ciphertext $y = 5$ from Bob.

- uses her private key to decrypt it.

$x = y^d \pmod{m}$

$x = 5^7 \pmod{33} = \boxed{14} \pmod{33}$

$5^7 = (5^3)^2 \cdot 5 = 125 \cdot 125 \cdot 5 = 15625 \cdot 5 = 78125$

$(-7)^2 \cdot 5 = 7 \cdot 2 = 14 \pmod{33}$

$5^7 = 5^2 \cdot 5^2 \cdot 5^2 \cdot 5 = 25 \cdot 25 \cdot 25 \cdot 5$

$25 \equiv -8 \pmod{33}$

$5^7 \pmod{33} \equiv (-8)(-8)(-8) \cdot 5 \equiv 64 \cdot (-25) \equiv 13 \cdot (-2) \equiv -26 \equiv 7$

$-64 \cdot 40 = 2 \cdot 7 = 14 \pmod{33}$

- receives the ciphertext $y = 17$

$D(17) = 17^7 \pmod{33} \equiv (-16)^7 \equiv -2^{28} \equiv -2^{20} \cdot 2^8 \equiv -2^8 \equiv -2^5 \cdot 2^3 \equiv (-32) \cdot 8 \equiv 8 \pmod{33}$