Suppose we use 30-digit primes for RSA cryptography.

p, q $\quad n = pq$

How many 30-digit primes are there?

about 10^{28} primes with 30 digits

Compare: Avogadro's number: 6×10^{23}

Total amount of disk space in the world: $\sim 10^{23}$ bytes

Total number of computer operations in history: $\sim 10^{26}$

Fermat's Little Theorem:

If p is prime and a is not divisible by p,
then $a^{p-1} \equiv 1 \pmod{p}$.

Testing whether p is prime:

- Choose some numbers $a_1, a_2, \ldots, a_k$ $\quad (k = 30)$
- For each, compute $a_i^{p-1} \pmod{p}$. If this is ever not 1, then p is not prime. If all $a_i^{p-1} \equiv 1 \pmod{p}$, then p is probably prime

MODULAR INVERSE:

The inverse of $a \pmod{n}$ is an integer b such that

$$ab \equiv 1 \pmod{n}.$$

GCD(a, n) is the greatest common divisor of a and n.

FACT: $GCD(a,n) = sa + tn$ for some s and t

example: $GCD(9, 24) = 3 = \underline{3} \cdot 9 + \underline{-1} \cdot 24$

Mathematica: ExtendedGCD[a,n] returns $\{g, \{s,t\}\}$

such that $GCD(a,n) = g = s \cdot a + t \cdot n$

If $GCD(a,n) = 1$, then $1 = s \cdot a + t \cdot n$

so: $1 \equiv s \cdot a \pmod{n}$

and thus, s is the multiplicative inverse of $a \pmod{n}$

RSA process:

- choose 30-digit primes p, q
- compute $n = p \cdot q$
- compute $\lambda = LCM(p-1, q-1)$
- choose an integer e relatively prime to λ
- compute $d = \text{modInverse}[e, \lambda]$

Public Key: (e,n) Private Key: (d,n)

Message: integer m, $0 \le m < n$

to encrypt m, you compute $c = m^e \pmod{n}$ (e: public key of the recipient; n: public key of the recipient; c: cypher)

to decrypt c, compute: $c^d \pmod{n}$

$$c^d = (m^e)^d = m^{ed} \equiv 1 \pmod{n}$$