How many 30-digit primes are there?

about 10^{28}

Compare: Avogadro's number: 6×10^{23}

Monster Group: 8×10^{53}

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

Total number of computer operations in history: maybe 10^{26}

Real RSA implementations use 250-digit primes.

Fermat's Little Theorem: If p is prime and a is not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

To determine if p is prime:

Choose $a_1, a_2, \ldots, a_k$, each smaller than p. ($k=30$)

For each, compute $a_i^{p-1} \pmod{p}$.

If I ever get a result $\neq 1$, then p is not prime.

If I always get 1, then p is probably prime.

MODULAR INVERSES:

Integers a and b are modular inverses $\pmod{n}$ if $a \cdot b \equiv 1 \pmod{n}$

example: 3 and 6 are inverses $\pmod{17}$

$3 \cdot 6 = 18 \equiv 1 \pmod{17}$

GCD: the greatest common divisor eg. $GCD(9,24) = 3$

FACT: $GCD(a,n)$ is a linear combination of a and n;
that is, $GCD(a,n) = s \cdot a + t \cdot n$ for some integers s, t

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

Mathematica: Extended GCD[a,n] returns $\{g, \{s,t\}\}$
where $gcd(a,n) = g = s \cdot a + t \cdot n$

Suppose: $GCD(a,n) = 1 = s \cdot a + t \cdot n$

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

s is inverse of $a \pmod{n}$

RSA Encryption:

- Choose primes p, q (30 digits each)
- Compute $n = p \cdot q$
- Compute $\lambda = LCM(p-1, q-1)$
- Choose encyption key e such that $GCD(e, \lambda) = 1$
- Compute $d = \text{modInverse}[e, \lambda]$

Public key: (e,n) — used to encrypt messages sent to you

Private key: (d,n) — used to decrypt messages sent to you