BIG NUMBERS

- How many 30-digit primes are there? about 10^{28}
- Avogadro's Number: 6×10^{23}
- Total amount of computer memory in the World:
  something like 10^{23} bytes
- Count of all computer instructions performed in history:
  maybe 10^{25}

Real RSA cryptography uses 200-digit numbers (or bigger).

FERMAT'S LITTLE THEOREM

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

Means that a^{p-1} and 1 have the same remainder mod p

That is: a^{p-1} is one more than a multiple of p.

APPLICATION: choosing primes

Let n be a (big) number. We want to know if n is prime.

Choose numbers $a_1, a_2, \ldots, a_m$ ($2 \le a_i < n$). For each, compute $a_i^{n-1} \pmod{n}$.

If n is prime, then $a_i^{n-1} \pmod{n}$ will always be 1.

If I find some a_i such that $a_i^{n-1} \pmod{n}$ is <u>not</u> 1, then n is <u>not</u> prime.

GREATEST COMMON DIVISOR (GCD)

Example: $GCD(12, 18) = 6$

GCD is a linear combination: $GCD(a, b) = sa + tb$ (integers)

Example: $3 = GCD(24, 9)$

$3 = (-1)24 + 3(9)$

MODULAR INVERSE

If $ab \equiv 1 \pmod{n}$, then a and b are <u>inverses</u> mod n.

How do we find the inverse of a mod n?

Find b such that $ab \equiv 1 \pmod{n}$.

Assume $\gcd(a, n) = 1$.

gcdExtended$[a, n]$ returns $\{g, s, t\}$

That is, $g = 1 = sa + tn$

So: $1 \equiv sa \pmod{n}$

Thus, s is the inverse of $a \pmod{n}$.