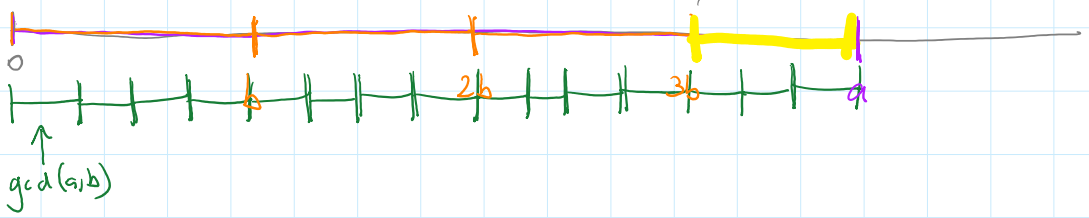
How many 30-digit prime numbers are there? 10^{28}

- Avogadro number: 6×10^{23}
- Total amount of computer memory in the world:
  something like 10^{22} or 10^{23} bytes
- Count of all computer instructions performed in history:
  maybe 10^{25}

Real RSA implementations use 200-digits (or more)

GCD – Euclidean Algorithm

$\gcd(a,b) = \gcd(b, a-3b)$



NOTE: GCD is a linear combination!

we can find s,t such that $sa + tb = GCD(a,b)$

example: $GCD(68, 12) = 4$ and $(-1)68 + 6(12) = 4$

$68 \div 12 = 5$ remainder 8

$12 \div 8 = 1$ remainder 4

$8 \div 4 = 2$ remainder 0

$8 = 68 \cdot 1 - 5 \cdot 12$

$4 = 12 \cdot 1 + 8$

$12 \cdot 1 - 4 = 68 \cdot 1 - 5 \cdot 12$

$-1(68) + 6(12) = 4$

RSA ENCRYPTION

1. Choose two prime numbers p, q (at least 30 digits)
   secret

2. Multiply: $n = pq$
   public

3. Compute totient: $\lambda(n) = \text{LCM}(p-1, q-1)$
   secret

4. Choose an encryption key: e (4 or more digits is good)
   public

5. Determine your decryption key: d = modular inverse of $e \pmod{\lambda}$
   secret

ENCRYPT: let m be a "message" i.e, a number

compute $c = m^e \pmod{n}$ ← use modPow 2

"cypher"

DECRYPT: compute $c^d = (m^e)^d = m^{ed} = m \pmod{n}$