Mathematics behind encryption of information

RSA, ASCII ..

primes

Number theory (Prime numbers)

Whole numbers, Integer numbers

$\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$ - set of integers

Def: $a, b \in \mathbb{Z}$ $\quad a \mid b$ 'a divides b' if

$\exists\, c \in \mathbb{Z}$ s.t.

there exists $\quad a \cdot c = b$ $\quad$ 'a is a divisor of b'

Ex: $6 \mid 18 \qquad 6 \cdot 3 = 18$

$10 \mid 10 \qquad 10 \cdot 1 = 10$

$7 \mid 0 \qquad 7 \cdot 0 = 0$

$3 \nmid 5$ ← does not divide

Properties of divisibility

- if $a \mid b$, $b \mid c \Rightarrow a \mid c$

Proof: $\underset{\mathbb{Z}}{\underset{\cap}{a \cdot d}} = b \qquad \underset{\mathbb{Z}}{\underset{\cap}{b \cdot f}} = c \qquad c = b \cdot f = a \cdot \underset{\mathbb{Z}}{\underset{\cap}{d \cdot f}}$

- $a \mid b \Rightarrow a^{100} \mid b^{100}$ $\quad$ ($n \in \mathbb{Z}_+ = \{1, 2, 3, 4, \dots\}$ positive integers)

$a \cdot d = b$, $d \in \mathbb{Z}$ $\qquad (a \cdot d)^{100} = b^{100}$

$a^{100} \cdot d^{100}$, $d^{100} \in \mathbb{Z}$

- if $a \mid x$, $a \mid y \Rightarrow a \mid m \cdot x + ny \quad \forall\, m, n \in \mathbb{Z}$

Proof: $\exists\, c, d \in \mathbb{Z}$ s.t.

$a \cdot c = x$, $a \cdot d = y$

$mx + ny = m \cdot a \cdot c + n \cdot a \cdot d = a(mc + nd)$ $\quad$ $mc+nd \in \mathbb{Z}$

Ex: $6 \mid 36$, $6 \mid 12$ $\Rightarrow 6 \mid 96$

$96 = 1 \cdot 36 + 5 \cdot 12$

Def: An even number x is $2 \mid x$

An odd number x is $2 \nmid x$

Theorem (Division algorithm)

Let $a, b \in \mathbb{Z}$, $b > 0$. Then $\exists$ unique $q, r \in \mathbb{Z}$ s.t. $a = b \cdot q + r$, $0 \le r < b$

Ex: $a = 100$, $b = 3$

$100 = 3 \cdot \underbrace{q}_{\text{quotient}} + \underbrace{r}_{\text{remainder}}$

$q = 33$
$r = 1$

Idea: increase q until $100 - 3 \cdot q$ becomes negative $\Rightarrow$ too far

Proof: First, find q, r, then prove uniqueness

Let $S = \{ a + by \mid y \in \mathbb{Z} \}$

$S^+ \subset S$ – subset of nonnegative numbers in S

Let r – the smallest element in S^+

$a = 100$, $b = 3$

$S = \{ -5, -2, 1, 4, 7, \underbrace{10}_{y=-30}, \dots, \underbrace{100}_{y=0}, 103, 106, \dots$

$S^+ = \{ \underbrace{1}_{r}, 4, 7, 10, \dots \}$

Claim: $0 \le r < b$ since $r \in S$ $r = a + by$ for some $y \in \mathbb{Z}$

$r \ge 0$ since $r \in S^+$

Suppose $r \ge b$: $r' = r - b = a + by - b = a + b(y-1) \ge 0$

$\Rightarrow r' \in S^+$

Contradiction, since r is the smallest element in S^+

$\Rightarrow r < b$

$r = a + by \Rightarrow a = r + b\underbrace{(-y)}_{q = -y}$

Now let us prove uniqueness

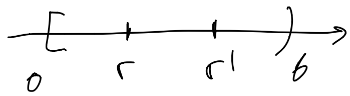
$\exists$ r, q; $r', q' \in \mathbb{Z}$ s.t.

$$-\begin{cases} a = bq + r, & 0 \le r < b \\ a = bq' + r', & 0 \le r' < b \end{cases}$$

$r, r' \in [0, b)$

$0 = a - a = bq + r - bq' - r' = b(q - q') + (r - r')$

$$6(q-q') = r'-r \Rightarrow 6 \mid r'-r$$



$\Downarrow$ $\qquad |r'-r| < 6 \qquad r'-r=0$, $r'=r$

$6(q-q')=0$, $6>0$

$q=q'$

Ex: Show that $5 \mid n^5-n \quad \forall n \in \mathbb{Z}_+$

base: $n=1$ ✓ $5 \mid 1^5-1 \quad 5 \mid 0$ true

$n=2 \quad 2^5-2 = 32-2=30 \quad 5 \mid 30$

$5 \mid 3^5-3$

If $5 \mid n^5-n \Rightarrow$

$n^5-n \equiv 0 \pmod 5$

Mathematical induction

assumption: Assume $\exists k \in \mathbb{Z}_+$ s.t. $5 \mid k^5-k$

Inductive step: $5 \mid (k+1)^5-(k+1)$

$$
\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & 1 & & 1 & & \\
 & 1 & & 2 & & 1 & \\
1 & & 3 & & 3 & & 1 \\
1 & 4 & & 6 & & 4 & 1 \\
\end{array}
$$

$n=5 \rightarrow 1 \; 5 \; 10 \; 10 \; 5 \; 1$

$$(k+1)^5-(k+1) = k^5+5k^4+10k^3+10k^2+5k+\cancel{1} - k - \cancel{1}$$

$$= \underbrace{k^5-k}_{5 \mid k^5-k} + \overbrace{5\underbrace{(k^4+2k^3+2k^2+k)}_{\in \mathbb{Z}}}^{\text{divisible by } 5}$$

By induction $5 \mid n^5-n \quad \forall n \in \mathbb{Z}_+$

$c \in \mathbb{Z}$

$n^5-n = 5 \cdot c$

$n=4$ ✓

$5 = 4+1$

$(4+1)^5-(4+1)$

$4^5-4 = 5 \cdot p$

Primes: Def A number $p \in \mathbb{Z}$ is prime if $p>0$ and has exactly two divisors: p and 1. Otherwise the number is called composite $\quad P = p_1^{k_1} p_2^{k_2} \cdots p_e^{k_e}$,

$e \in \mathbb{Z}$

$k_1, \dots, k_e \in \mathbb{Z}_+$

~~1~~ $\quad 2, 3, 5, 7, 11, 13, 17, 19, 23 \dots$

94 049

1299 709 ...

The largest known prime: $2^{74,207,281}-1 \sim 10^{21\,000\,000}$

$2^{50} \sim 10^{15} \qquad \log_{10} 2 = \dfrac{\log 2}{\log 10} \simeq 0.301$

$\pi(x) = \#$ primes $< x$

$\pi(10) = 4$
$\pi(20) = 8$
$\pi(100) = 25$

$$\frac{100}{\log 100} \simeq \frac{100}{4.6} \simeq 22$$

$$\pi(x) \approx \frac{x}{\log x}, \quad x \to \infty$$

Finding primes (Sieve of Eratosthenes)

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~ $= N$

- cross out all multiples of 2 except 2
- circle the first non-crossed number
- do over

Need to iterate roughly $\sqrt{N}$ times

Why: If $a > \sqrt{N}$ $\quad a = 6, 7, 8 \ldots$

$K < N$ $\quad a \mid K$ $\quad$ is K already crossed out?

$a \mid K \Rightarrow K = a \cdot c, \; c \in \mathbb{Z}$ $\quad c \mid K$

$K < N, \; a > \sqrt{N} \Rightarrow c < \sqrt{N}$

then K is a multiple of c and it had been crossed out.

Fun HW: Write a code which calculates the largest prime possible on your machine.

Primes: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$

Gaps: 1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6 ← Congruent to 1

$4k+1$: $5, 13, 17, 29$ $\quad \equiv 1 \pmod 4$

$4k+3$: $3, 7, 11, 19, 23 \ldots$ $\quad \equiv 3 \pmod 4$

Theorem: There are infinitely many primes.

Idea: $a \mid b, \; a > 1 \Rightarrow a \nmid b+1$ $\quad 6 \mid 12 \quad 6 \nmid 13$ $\quad 7 \mid 21 \quad 7 \nmid 22$

$\exists \; c \in \mathbb{Z}$ s.t. $b = a \cdot c$

assume $a \mid b+1 \Rightarrow \exists \, d \in \mathbb{Z}$ s.t. $b+1 = a \cdot d$

$$1 = (b+1) - b = a \cdot d - a \cdot c = a(\underbrace{d-c}_{\in \mathbb{Z}})$$

$\Rightarrow a \mid 1$ impossible unless $a = 1$.

<u>Proof of the theorem:</u> Assume there are finitely many primes

$\mathcal{P} = \{ p_1, p_2, \dots, p_k \}$ – complete list of all primes

consider $N = p_1 \cdot p_2 \cdots p_k$, look at $N+1$

by construction $p_1 \mid N$, $p_2 \mid N, \dots, p_k \mid N$

but $p_1 \nmid N+1$, $p_2 \nmid N+1, \dots, p_k \nmid N+1$

Does $N+1$ have any divisors? Yes $1, N+1$ if there are no others

then $N+1$ is prime

if there are: $N+1 = a \cdot b$, $a, b < N+1$

$a \mid N+1$.

Is a prime? Yes, No: $a = c \cdot d$

$c, d < a$

is c prime? Yes, No: $c = e \cdot f$

$\vdots$ $\vdots$

this process will terminate when we find a prime

$p \mid N+1$

but $p \notin \mathcal{P}$ $\Rightarrow$ $\mathcal{P}$ does not contain all primes

<u>Proposition:</u> Given any $N \in \mathbb{Z}_+$ there are two <u>consequtive</u> primes which are $\geq N$ apart.

$\underbrace{p-1, p, p+1 \dots\dots p'-1, p'}_{\geq N}, p'+1$

$p - p' \geq N$

$(n+1)! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n \cdot (n+1)$ $\leftarrow (i+1)$

<u>Proof:</u> $n = N-1$: $a_i = (n+1)! + i+1$, $i = 1 .. n$

$n = N-1$ of composite numbers $\Leftarrow$ $\begin{cases} a_1 = (n+1)! + 2 \\ a_2 = (n+1)! + 3 \\ \vdots \\ a_n = (n+1)! + (n+1) \end{cases}$

$n = 10$

$a_1 = 11! + 2 = 481,466,702$

$a_2 = 11! + 3 = 481,466,703$

$\vdots$

$a_{10} = 481,466,711$

$(i+1) \mid a_i \quad \forall \; 1 \leq i \leq n$

$a_i = (i+1)\left(\frac{(n+1)!}{i+1}+1\right)$ all a_i's are composite (not prime)

Next time: Modular arithmetic, Little Fermat theorem, Euler's theorem, RSA encryption

The Fundamental theorem of Arithmetic ($\mathbb{Z}$)

For every $N>1$ $\exists$ a prime factorization of N:

$\exists$ distinct primes $p_1, p_2, \dots p_k$, $r_1 \dots r_k$, $r_i \geq 1$, $i=1,\dots k$

s.t. $N = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$

The factorization is unique up to reordering of the factors.

Ex: Complex numbers $a+\sqrt{-5}\,b$ $(\sqrt{-5})^2 = -5$

(Gaussian primes) $\mathbb{Z} \subset \mathbb{Z}[\sqrt{-5}] = \{ a+b\sqrt{-5} \mid a,b \in \mathbb{Z} \}$

- $(1+\sqrt{-5})(1-\sqrt{-5}) = 1\cdot 1 - \sqrt{-5}\cdot\sqrt{-5} = 6$

- $2 \cdot 3 = 6$