$\phi(N)$

Definition

For $N \in \mathbb{N}$ we define $\phi(N) = |\mathbb{Z}_N^*|$.

Example

- $\phi(N) = \boxed{N - 1}$ if N is prime.
- $\phi(15) =$. $|\{1, 2, 4, 7, 8, 11, 13, 14\}| = 8$

Recap: Rings

A set R is a *ring* if it has two binary operations, written as addition and multiplication, such that for all $a, b, c \in R$

(R1) $a + b = b + a \in R$

(R2) $(a + b) + c = a + (b + c)$

(R3) There exists an element $0 \in R$ with $a + 0 = a$

(R4) There exists an element $-a \in R$ with $a + (-a) = 0$

$(R, +)$ IS AN ABELIAN GROUP

(R5) $a(bc) = (ab)c$

(R6) There exists an element $1 \in R$ with $1 \cdot a = a \cdot 1 = a$

SOME ELEMENTS MAY NOT HAVE A MULTIPLICATIVE INVERSE

(R7) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

Recap: Rings

Examples:

- $\mathbb{Z}$
- $\mathbb{Z}_N$
- $R_1 \times \cdots \times R_k$, where $R_1, \ldots, R_k$ are rings.

HERE
$(x_1, x_2, \ldots, x_k) + (y_1, y_2, \ldots, y_k) = (x_1+y_1, \ldots, x_k+y_k)$
SIMILARLY FOR "·"

- The set of $n \times n$ matrices over $\mathbb{Z}$ with the standard matrix addition and multiplication.

$\mathbb{0} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \quad \mathbb{1} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

Example of an easy ring-theorem

Theorem

Let R be a ring, then for each $r \in R$ one has

$$0 \cdot r = 0 = r \cdot 0.$$

Ring homomorphism

If R and R_1 are rings, a mapping $\theta : R \to R_1$ is called a *ring homomorphism* if for all $r, s \in R$:

(1) $\theta(r+s) = \theta(r) + \theta(s)$

(2) $\theta(rs) = \theta(r) \cdot \theta(s)$ R R₁ WE OMIT TO REMARK WHICH RING WE ARE IN

(3) $\theta(1_R) = 1_{R_1}$

Examples:

A ▸ $f : \mathbb{Z} \to \mathbb{Z}_N$, $f(x) = [x]_N$

B ▸ $g : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}_N$, $f(x) = (x, [x]_N)$.

A (1) $f(r+s) \overset{?}{=} f(r) + f(s) = \big[[r]_N + [s]_N\big]_N$

$[r+s]_N = [\alpha N + \tilde{r} + \beta N + \tilde{s}]_N = [\tilde{r} + \tilde{s}]_N$

$r = \alpha N + \tilde{r}$, $s = \beta N + \tilde{s}$

(2), (3): SIMILARLY EASY

B FOLLOWS FROM:

IF $f_i : R \to R_i$ HOMOMORPHISM

$g : R \to (R_1 \times R_2 \times \dots \times R_k)$

IS A RING HOMOMORPHISM

Chinese remainder theorem

EXAMPLES

$a = 10,\ b = 5 \to$ NOT COPRIME ✗

$a = 10,\ b = 7$ ✓

$f(41) = (1, 6)$

$f(38) = (3, 3)$

$f(19) = (9, 5)$

Theorem

Suppose a and b are relatively prime integers. Then the map

$$\begin{array}{rccc} f: & \mathbb{Z}_{a\cdot b} & \to & \mathbb{Z}_a \times \mathbb{Z}_b \\ & [x]_{a\cdot b} & \mapsto & ([x]_a, [x]_b) \end{array}$$

is a ring isomorphism, that is, a ring homomorphism that is also a bijection.

PF.

✓ (I) PROVE THAT IT IS AN HOMOMORPHISM

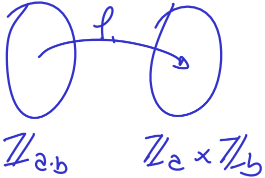
$$f(r+s) \overset{?}{=} f(r) + f(s) = \left(\left[[r]_a + [s]_a \right]_a, \left[[r]_b + [s]_b \right]_b \right)$$

$$\parallel$$

$$\left([r+s]_a, [r+s]_b \right)$$

AND WE ALREADY SAW $[r+s]_a = \left[[r]_a + [s]_a \right]_a$

SIMILARLY (II), (III) FOLLOW FROM LAST PAGE



Theorem

Suppose a and b are relatively prime integers. Then the map

$$\begin{array}{rccc} f: & \mathbb{Z}_{a\cdot b} & \to & \mathbb{Z}_a \times \mathbb{Z}_b \\ & [x]_{a\cdot b} & \mapsto & ([x]_a, [x]_b) \end{array}$$

is a ring isomorphism, that is, a ring homomorphism that is also a bijection.

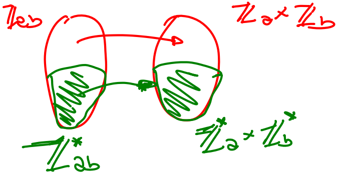
② SHOW THAT f IS A BIJECTION.

AS $|\mathbb{Z}_{a,b}| = a\cdot b = |\mathbb{Z}_a|\cdot|\mathbb{Z}_b|$, IT IS ENOUGH TO SHOW THAT f IS SURJECTIVE

LET $(p,r) \in \mathbb{Z}_a \times \mathbb{Z}_b$. AS $\gcd(a,b)=1 \Rightarrow \exists\, x,y \in \mathbb{Z} : ax+by=1$

LET $q = [rax+pby]_{ab}$. THEN $[q]_a = [rax+pby]_a = [pby]_a = [p(1-ax)]_a = p$

SIMILARLY $[q]_b = r$



THE BIJECTION f INDUCES A BIJECTION BETWEEN $\mathbb{Z}^*_{ab}$ AND $\mathbb{Z}^*_a \times \mathbb{Z}^*_b$

Corollary

If $a, b \in \mathbb{N}$ and $\gcd(a, b) = 1$, then $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

PF.

$\phi(a \cdot b) = |\mathbb{Z}^*_{ab}|$, $\phi(a) = |\mathbb{Z}^*_a|$, $\phi(b) = |\mathbb{Z}^*_b|$

Let $x \in \mathbb{Z}_{ab}$. Then

$x \in \mathbb{Z}^*_{ab} \iff \gcd(x, ab) = 1$

$\iff \exists\, y_x : \; x \cdot y_x \equiv 1 \bmod ab$

$\iff f(x) \cdot f(y_x) = f(x\, y_x) = f(1) = (1, 1)$

$\iff$ x_1 HAS AN INVERSE IN $\mathbb{Z}_a$, WHERE $f(x) = (x_1, x_2)$
x_2 " $\mathbb{Z}_b$

$\iff x_1 \in \mathbb{Z}^*_a, \; x_2 \in \mathbb{Z}^*_b$

$\Rightarrow |\mathbb{Z}^*_{ab}| = |\mathbb{Z}^*_a| \cdot |\mathbb{Z}^*_b| \quad \square$

$\phi(\cdot)$ and factoring

Corollary

Let $N = p_1^{e_1} \cdots p_k^{e_k}$ be the factorization of N into distinct prime numbers $p_1, \ldots, p_k$, then

$$\phi(N) = \prod_{i=1}^{k} (p_i - 1) \cdot p_i^{e_i - 1}$$

PF.

PREVIOUS PAGE

$$\phi(N) = \prod_{i=1}^{k} \phi(p_i^{e_i})$$

$$\phi(p_i^{e_i}) = \left| \mathbb{Z}^*_{p_i^{e_i}} \right| = \left| \{1, 2, \ldots, p_i - 1, \cancel{p_i}, p_i + 1, \ldots, 2p_i - 1, \cancel{2p_i}, 2p_i + 1, \ldots, p_i^{e_i} - 1, \cancel{p_i^{e_i}}\} \right|$$

$$= p_i^{e_i} - p_i^{e_i - 1} = p_i^{e_i - 1}(p_i - 1)$$

$\blacksquare$

POINTS WE SKIPPED

$1 \cdot p_i, 2 \cdot p_i, \ldots, p_i^{e_i - 1} \cdot p_i$

RSA

ALICE WANTS TO SEND A MESSAGE TO BOB BUT THEY KNOW THAT ALL THEY SAY MAY BE INTERCEPTED BY EVE

(RIVEST, SHAMIR, ADLEMAN 77)

EFFICIENT ALGORITHMS

Bob:

- Generates large (4000 bits) primes p and q → ? WE WILL SEE LATER
- Computes $N = p \cdot q$.
- Selects *encryption exponent* e such that $\gcd(e, \underbrace{\phi(N)}_{=(p-1)(q-1)}) = 1$ → EXTENDED EUCLIDEAN ALG
- Public key: (N, e)

EVERYBODY KNOWS (INCLUDING EVE)

Alice:

- Converts message to bit-string m
- Sends $s = m^e \pmod{N}$ to Bob → FAST MODULAR EXPONENT.

Bob:

- Computes $y = e^{-1} \pmod{\phi(N)}$ → EEA
- Computes $s^y \equiv m \pmod{N}$. → FME

RSA

IF EVE KNEW HOW TO FACTORIZE A NUMBER, THEN:
→ SHE RECOVERS p, q FROM N
⇒ SHE RECOVERS $\phi(N)$
⇒ SHE RECOVERS y ⇒ SHE DECODES s AND GET m BACK.
BUT WE DO NOT KNOW ALGORITHMS TO EFFICIENTLY FACTORIZE A NUMBER

Bob:

- Generates large (4000 bits) primes p and q
- Computes $N = p \cdot q$.
- Selects *encryption exponent* e such that $\gcd(e, \phi(N)) = 1$
- Public key: (N, e)

Alice:

- Converts message to bit-string m
- Sends $s = m^e \pmod N$ to Bob

Bob:

- Computes $y = e^{-1} \pmod{\phi(N)}$
- Computes $\boxed{s^y \equiv m \pmod N}$

WE NEED TO PROVE IT.

$s^y = m^{e \cdot y} = m^{1 + k\phi(N)} = m^{1 + k(p-1)(q-1)}$

CASE 1: $p \nmid m$

$s^y = m \cdot \underbrace{m^{k(p-1)(q-1)}}_{\equiv 1 \bmod p} \equiv m \cdot 1 \equiv m \bmod p$ [FERMAT'S LITTLE THR.]

CASE 2: $p \mid m$, SAY $m = cp$

$s^y = (cp)^y \equiv 0 \equiv m \bmod p$

IN BOTH CASES, $s^y - m \equiv 0 \bmod p$. SIMILARLY $s^y - m \equiv 0 \bmod q$

$\Rightarrow s^y - m \equiv 0 \bmod \underbrace{(p \cdot q)}_{N}$ ∎

Implementing RSA: Two guiding questions

A) How to recognize prime numbers? PRIMALITY TEST

B) Are the prime numbers dense enough such that a random *n*-bit number is a prime with reasonable probability? PRIME NUMBER / CHEBYSHEV THR

HOW TO GENERATE PRIME NUMBERS ?

- SELECT A RANDOM NUMBER AND CHECK IF IT IS PRIME
  IF NOT, REPEAT.

FOR THIS ALGORITHM TO WORK, WE NEED TO ANSWER A), B) ABOVE

Primality tests

- Weak Fermat test
- Charmichael numbers
- The Miller-Rabin test

THEY FOOL THE WEAK FERMAT TEST
BUT NOT THE MILLER-RABIN TEST

RANDOMIZED TESTS
- ANSWER IS ALWAYS CORRECT IF INPUT NUMBER IS PRIME
- ANSWER IS WRONG WITH BOUNDED PROBABILITY IF INPUT NUMBER IS COMPOSITE

DETERMINISTIC, EFFICIENT PRIMALITY TEST EXISTS
[AKS, 2004]

The weak Fermat test

- Input: $N \in \mathbb{N}$ odd
- Assert: *Composite* or *probably prime*
- Choose $a \in \{1, \ldots, N-1\}$ uniformly at random
- If $a^{N-1} \pmod N = 1$ assert *probably prime*
- else assert *composite*

IF N IS PRIME, BY FLT THE ANSWER IS ALWAYS "PROBABLY PRIME"

An odd composite number $N \in \mathbb{N}$ is called *Carmichael number* if

$$\underbrace{\forall a \in \mathbb{Z}_N^*\colon\ a^{N-1} = 1}_{\text{FOR ALL THOSE } a\text{, THE WFT IS FOOLED}}.$$

If N is not Carmichael

Theorem

Let N be an odd composite number that is not Carmichael, then the weak Fermat test asserts probably prime with probability at most $1/2$.

If the weak Fermat test is repeated i times, then the probability that it asserts probably prime in all i rounds is at most $1/2^i$.

PF.

- Let $H = \{ a \in \mathbb{Z}_N^* : a^{N-1} = 1 \bmod N \}$ ← EXACTLY THE SET THAT FOOLS THE FERMAT TEST (I.E. THAT MAKE IT ANSWER "PROBABLY PRIME" EVEN IF N IS COMPOSITE)
- AS N IS NOT CARMICHAEL $\Rightarrow (*)\ H \subsetneq \mathbb{Z}_N^*$
- $H \trianglelefteq \mathbb{Z}_N^*$ [EASY EXERCISE]

BY LAGRANGE THEOREM, $|H| \cdot t = |\mathbb{Z}_N^*|$ FOR SOME $t \in \mathbb{N}$. FROM $(*) \Rightarrow t \geq 2$

$\Rightarrow |H| = \frac{1}{t} |\mathbb{Z}_N^*| \leq \frac{1}{2} |\mathbb{Z}_N^*| \leq \frac{1}{2} |\mathbb{Z}_N| \Rightarrow P\left[\begin{array}{l}\text{ALGORITHM}\\ \text{IS FOOLED}\end{array}\right] \leq \frac{1}{2}$

SET OF a THAT WILL FOOL THE ALGORITHM (ON INPUT N)

SET OF ALL POSSIBLE a

How do Carmichael numbers look like

Theorem

Every Carmichael number N is of the form

$$N = p_1 \cdots p_k,$$

where the p_i are distinct primes and $(p_i - 1) \mid (N - 1)$ for $i = 1, \ldots, k$.