HC 9

Proposition: assume $a^s = a^t$, $s < t \leq n$

$\Rightarrow a^{t-s} = a^{s-s} = a^0 = e$ but $t-s < n$ ↯

- $k \in \mathbb{Z}$ arbitrary, then

$a^k = a^{qn+r}$ $(k = qn+r,\ 0 \leq r < n)$

$= (a^n)^q a^r = a^r \in \{a, a^2, \ldots, a^n\}$ ∎

Claim: $\langle a^k \rangle = \langle a \rangle \iff \gcd(k,n) = 1$

(1)

Pf: „$\Rightarrow$" $\langle a^k \rangle = \langle a \rangle \Rightarrow \exists s : (a^k)^s = a$

$\Rightarrow k \cdot s = 1 \pmod n$

$\Rightarrow \gcd(k,n) = 1$

„$\Leftarrow$" $\gcd(k,n) = 1 \Rightarrow 1 = s \cdot k - t \cdot n$, $s,t \in \mathbb{Z}$

$\Rightarrow (a^k)^s = a\,(a^n)^t = a$

$\Rightarrow \langle a \rangle \subseteq \langle a^k \rangle$

Also, $\langle a^k \rangle \subseteq \langle a \rangle$ by definition ∎

HC 9

$$\boxed{\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \quad , \quad n = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}}$$

PF: (i) $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ [if a, b coprime]

write all numbers $1, \ldots, a \cdot b$ in

1	$b+1$	$\cdots$	$(a-1)b+1$
2	$b+2$		$(a-1)b+2$
$\vdots$	$\vdots$		$\vdots$
b	$2b$		ab

(2)

row k: $k, b+k, \ldots, (a-1)b+k$ } a numbers

- if $d = \gcd(b,k) > 1$, then d divides ab and all numbers in row k $\Rightarrow$ none is coprime with ab

- if $\gcd(b,k) = 1$, then all are coprime with b, and as $\gcd(a,b) = 1$, exactly $\phi(a)$ numbers of $k, b+k, \ldots, (a-1)b+k$ are coprime with a, (*) next page hence also with ab.

$\Rightarrow \phi(ab) = \phi(b) \cdot \phi(a)$ ∎

(ii) count numbers not coprime with p^e:

$\underbrace{p, 2p, 3p, \ldots, p^2}_{p}, \underbrace{p^2+p, \ldots 2p^2, \ldots, p^3, \ldots p^e}_{p \cdot p = p^2}$ ⋮ p^{e-1}

$\Rightarrow \phi(p^e) = p^e - p^{e-1} = p^e\left(1 - \frac{1}{p}\right)$ ∎

HC 9 (*)

The # of coprimes of a in $\{1,\dots,a\}$ is $\phi(a)$ by definition of $\phi(\cdot)$.

Claim: The # of coprimes of a in $\{k, k+1, \dots, k+a-1\}$, and also in $\{k, b+k, 2b+k, \dots, (a-1)b+k\}$ is $\phi(a)$, too, if $\gcd(a,b)=1$, for any $k \in \mathbb{Z}$.

Example: $a=4$, $b=5$, $k=2$

Then $\{k,\dots,k+a-1\} = \{2,3,4,5\}$, which is the same as $\{2,3,4,1\} \pmod 4$.

(2a) And $\{k, b+k, 2b+k, \dots, (a-1)b+k\} = \{2,7,12,17\}$, which is the same as $\{2,3,4,1\} \pmod 4$.

Proof: Let $\ell \in \{1,\dots,a\}$, and let $f(\ell) := (\ell-1)b + k \pmod a$, then $f\{1,\dots,a\} \to \{1,\dots,a\}$ is bijective: take any $\ell \neq \ell'$, then $f(\ell) = f(\ell')$ implies $\ell = \ell'$, as

$$(\ell-1)b + k = (\ell'-1)b + k \pmod a$$
$$\Leftrightarrow (\ell-1)b = (\ell'-1)b \pmod a$$
$$\Rightarrow (\ell-1) = \ell'-1 \pmod a$$
$$\Leftrightarrow \ell = \ell', \pmod a$$

As $\gcd(a,b)=1$ $\Rightarrow$ b has inverse for "$\cdot$" in $\mathbb{Z}_a$

As f is injective, $|f(\{1,\dots,a\})| = a$, so f is surjective, too.

As $\{1,\dots,a\} = \{k,\dots,(a-1)b+k\} \pmod a$, the claim follows ∎

HC 9

$\varphi(p) = p-1$: coprimes $= 1, \dots, p-1$

$\varphi(pq) = (p-1)(q-1)$:

not coprime are $p, 2p, \dots, qp$ } q numbers

$q, 2q, \dots, pq$ } p numbers

$\Rightarrow \varphi(pq) = pq - (p+q-1) = (p-1)(q-1)$ ∎

Consequences Lagrange

(3)

(1) ✓

(2) take $a \neq e$, then $|\langle a \rangle| \geq 2$, as $|\langle a \rangle| \mid n$

and n = prime, $|\langle a \rangle| = n \Rightarrow \langle a \rangle = G$ ∎

(3) say $|\langle a \rangle| = m$, then $m \mid n$, so $n = km$

$a^n = (a^m)^k = e$ ∎

Proof Euler

$\gcd(M, n) = 1 \Rightarrow M \in U_n$ [∃ mult. inverse]

Now $|U_n| = \varphi(n)$ so $M^r = M^{\varphi(n)} = 1 \pmod n$

[proof here for $M \in U_n$, but even true for

all $M \in \mathbb{Z}$! Ex. RSA.4]

HC9

RSA example

Alice: $\varphi(n) = \varphi(3 \cdot 11) = 2 \cdot 10 = 20$
(p, q)

$\gcd(7, 20) = 1$ (as $1 = 3 \cdot 7 - 20$)

$\Rightarrow 7^{-1} = 3 \pmod{20}$

or $3 \cdot 7 = 1 \pmod{20}$

or $3 \cdot 7 = 1 + 20$

(4)

in general, compute by extended Euclid. Alg.:

$$\begin{pmatrix} 20 & 1 & 0 \\ 7 & 0 & 1 \end{pmatrix} \quad 20 = 1 \cdot 20 + 0 \cdot 7, \quad 7 = 0 \cdot 20 + 1 \cdot 7$$

$$\hookrightarrow \begin{pmatrix} 6 & 1 & -2 \\ 7 & 0 & 1 \end{pmatrix} \quad 6 = 1 \cdot 20 - 2 \cdot 7$$

$$\hookrightarrow \begin{pmatrix} 6 & 1 & -2 \\ 1 & -1 & 3 \end{pmatrix} \quad 1 = -20 + 3 \cdot 7$$

$\Rightarrow \gcd(20, 7) = 1$ and $7^{-1} = 3$

Bob: $C = M^e = 8^7 \pmod{33}$

$= (8^2)^3 \cdot 8 \pmod{33}$

$= (64)^3 \cdot 8 \pmod{33}$

$= (-2)^3 \cdot 8 \pmod{33}$

$= -64 \pmod{33}$

$= 2 \pmod{33}$

Alice: $M = C^d = 2^3 = 8$ ∎

HC 9

Modular exponentiation

Compute $8^7 \pmod{33}$

$$8^7 = 8^1 \cdot 8^2 \cdot 8^4$$
$$= 8^{2^0} \cdot 8^{2^1} \cdot 8^{2^2}$$
$$= 8^{2^0} \cdot (8^{2^0})^2 \cdot (8^{2^1})^2$$

Now use that $(a \cdot b) \pmod{n} = a \pmod{n} \cdot b \pmod{n}$

$8^{2^0} = 8 \pmod{33}$

$8^{2^1} = (8^{2^0})^2 = 8^2 = 64 = 31 \pmod{33}$

(5)

$8^{2^2} = (8^{2^1})^2 = (31)^2 = 961 = 4 \pmod{33}$

$\Rightarrow 8^7 = 8 \cdot 31 \cdot 4 \pmod{33}$
$= 8 \cdot 124 \pmod{33}$
$= 8 \cdot 25 \pmod{33}$
$= 200 \pmod{33}$
$= 2 \pmod{33}$ ☒