§ 4 A Glimpse of Number Theory

Number Theory : Study of numbers (usually means integers)

Definition 4.1

Let $a, b \in \mathbb{Z}$, we say a divides b (denoted by $a|b$) if $b = ac$ for some $c \in \mathbb{Z}$.

In this case, a is said to be a divisor of b.

Example 4.1

$2|6$, $3|6$, $-3|6$, $3|-6$, but $4 \nmid 6$

$n|0$ for all integers n (A little bit odd to have $0|0$)

Definition 4.2

An integer $n > 1$ is said to be a prime if the only positive divisors of n are 1 and n, otherwise n is called a composite.

Remark : The number 1 is neither prime nor composite.

Example 4.2

First few primes : $2, 3, 5, 7, 11, 13, 17, 19, \cdots$

First few composites : $4, 6, 8, 9, 10, 12, 14, 15, \cdots$

Definition 4.3

Let $a, b \in \mathbb{Z}$. The greatest common divisor (gcd) of a and b is defined by

$$\gcd(a,b) = \begin{cases} \max\{d \in \mathbb{Z} : d|a \text{ and } d|a\} & \text{if not both } a, b \text{ are } 0 \\ 0 & \text{if } a = b = 0 \end{cases}$$

Remark : $\gcd(a, 0) = |a|$

Example 4.3

Divisors of 18 : $\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18$

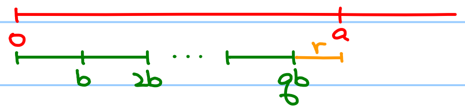
Divisors of -12 : $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$

$\gcd(18, -12) = 6$

Question: How to find gcd(a,b) if both a and b are large?

Theorem 4.1 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b \neq 0$ Then there exists unique $q, r \in \mathbb{Z}$ such that $0 \leq r < |b|$ and $a = bq + r$.



Lemma 4.1

$\gcd(a,b) = \gcd(b,r)$.

proof:

If $d = \gcd(a,b)$, then $d \mid a$ and $d \mid b$.

Therefore, $d \mid a - bq = r$.

$d \mid b$ and $d \mid r$ (d is a common divisor of b and r) $\Rightarrow d \leq \gcd(b,r)$

If $d' = \gcd(b,r)$, then $d' \mid b$ and $d' \mid r$.

Therefore, $d' \mid bq + r = a$

$d' \mid a$ and $d' \mid b$ (d is a common divisor of a and b) $\Rightarrow d' \leq \gcd(b,r)$

$\therefore \gcd(a,b) = \gcd(b,r)$.

Example 4.4 (Euclidean Algorithm)

Find gcd(240,168)

$240 = 1 \times 168 + 72$ $\quad \gcd(240,168) = \gcd(168,72)$

$168 = 2 \times 72 + 24$ $\quad \gcd(168,72) = \gcd(72,24)$

$72 = 3 \times 24$ $\quad \gcd(72,24) = 24$

$\therefore \gcd(240,168) = 24$

Exercise 4.1

Find gcd(817, 1247).

Ans: 43

Theorem 4.2

Let $a, b \in \mathbb{Z}$. There exists $s, t \in \mathbb{Z}$ such that $as + bt = \gcd(a,b)$.

Example 4.5 (Extended Euclidean Algorithm)

$284 = 4 \times 68 + 12$

$68 = 5 \times 12 + 8$

$12 = 1 \times 8 + 4$

$8 = 2 \times 4$

$$\begin{aligned}
\gcd(284, 68) = 4 &= 12 - 1 \times 8 \\
&= 12 - 1 \times (68 - 5 \times 12) \\
&= 6 \times 12 - 1 \times 68 \\
&= 6 \times (284 - 4 \times 68) - 1 \times 68 \\
&= 6 \times 284 - 25 \times 68
\end{aligned}$$

Definition 4.4

Let $a, b \in \mathbb{Z}$. a and b are said to be relatively prime if $\gcd(a,b) = 1$.

Example 4.6

bucket with unknown volume | glass 37 mL | cup 78 mL | water tap

Question: What should we do so that at the end we have 1 mL of water in the bucket?

By extended Euclidean Algorithm, $\gcd(37, 78) = 1 = 19 \times 37 - 9 \times 78$

Exercise 4.2

Let $a, b, c \in \mathbb{Z}$. Prove that

There exists $s, t \in \mathbb{Z}$ such that $as + bt = c$ if and only if $\gcd(a,b) \mid c$.

Lemma 4.2

Let $n, a, b \in \mathbb{Z}$ such that $n \mid a$ and $n \mid b$, then $n \mid \gcd(a,b)$

proof:

$n \mid a$ and $n \mid b \Rightarrow a = np$ and $b = nq$ for some $p, q \in \mathbb{Z}$.

There exist $s, t \in \mathbb{Z}$ such that $\gcd(a,b) = as + bt$

$= n(ps + qt)$ where $ps + qt \in \mathbb{Z}$.

$\therefore n \mid \gcd(a,b)$

Proposition 4.1

Let $a, b \in \mathbb{Z}$ and let p be a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

proof:

Suppose that $p \mid ab$.

If $p \mid a$, it's done!

If $p \nmid a$, since p is a prime, we have $\gcd(a,p) = 1$.

Then, there exist $s, t \in \mathbb{Z}$ such that $1 = as + pt$

$$b = abs + ptb$$

$$b = pqs + ptb \qquad p \mid ab \Rightarrow ab = pq \text{ for some } q \in \mathbb{Z}.$$

$$b = p(qs + tb)$$

$$\therefore p \mid b$$

Theorem 4.3 (Prime Factorization)

Every positive integer greater than 1 can be expressed as a product of primes in a unique way

proof:

Let S be the set of all positive integers greater than 1 which cannot be expressed as a product of primes.

Suppose the contrary Then S is a nonempty set of $\mathbb{N}$.

By well ordering principle, S has a least element m. Firstly, m cannot be a prime, so $m = ab$ for some positive integers a, b with $a, b < m$.

Therefore, $a, b \notin S$, i.e. a and b can be expressed as a product of primes, but then $m = ab$ which can be expressed as a product of primes. (Contradiction)

$\therefore$ Every positive integer greater than 1 can be expressed as a product of primes.

Suppose that n is a positive integer greater than 1 and $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ where p_i's and q_i's are primes.

By proposition 4.1, $p_1 \mid q_1 q_2 \cdots q_s \Rightarrow p_1 \mid q_i$ for some i

but q_i itself is a prime, so $q_i = p_1$

By swapping the index, we let $q_1 = p_1$ and we have $p_2 \cdots p_r = q_2 \cdots q_s$

Repeating the above, we have $r = s$ and $p_i = q_i$ for $i = 1, 2, \cdots, r$

$\therefore$ n can be expressed as a product of primes a unique way.

Primes : "Elements" of numbers !

Exercise 4.3

Let $a, b, c \in \mathbb{Z}$. Show that if $c \mid ab$ and $\gcd(a,c) = 1$, then $c \mid b$

Some Results / Questions of Number Theory :

1) Question : How many primes ?

Theorem 4.4

There are infinitely many primes.

2) Question : Given a positive integer n, how many primes $\leq n$ are there ?

Let $\pi(n) = |\{p \in \mathbb{N}^+ : p \leq n \text{ is a prime}\}|$.

Theorem 4.5

$$\lim_{n \to \infty} \frac{\pi(n)}{\left(\frac{n}{\ln(n) - 1}\right)} = 1$$

Think : $\pi(1000) = 168 \approx \frac{1000}{\ln(1000) - 1} \approx 169.27$

3) Twin primes : both p and $p+2$ are primes, e.g. $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$

Question : Are there infinitely many pairs of twin primes ?

Not yet known (Twin prime conjecture)

4) Note. $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, $7^2 + 24^2 = 25^2$

Question : Given an integer $n > 2$, are there positive integers a, b, c such that

$$a^n + b^n = c^n \quad ?$$

Answer : No ! (Fermat Last Theorem)

The Ring of Integers Modulo n

Definition 4.5

Let n be a positive integers.

If $a, b \in \mathbb{Z}$ such that $n \mid b-a$, then we say a is congruent to b modulo n.

and it is denoted by $a \equiv b \pmod{n}$

Remark. "|" defines an equivalence relation $\sim$ on $\mathbb{Z}$ ($a \sim b$ if $n \mid b-a$)

Proposition 4.2

If $a \equiv a' \pmod{n}$, $b \equiv b' \pmod{n}$, then $a+b \equiv a'+b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$

(Define $\sim$ on $\mathbb{Z}$ so that $a \sim b$ if $n \mid b-a$. The above proposition means

If $a \sim a'$ and $b \sim b'$, then $a+b \sim a'+b'$ and $ab \sim a'b'$.

Addition and multiplication on $\mathbb{Z}$ induce addition and multiplication on $\mathbb{Z}/\sim = \mathbb{Z}_n$.)

Example 4.7

$23 \equiv 2 \pmod{7}$, $34 \equiv 6 \pmod{7}$

$23 + 34 \equiv 2+6 \equiv 8 \equiv 1 \pmod{7}$ (Compare to $23+34 = 57 \equiv 1 \pmod{7}$)

$23 \times 34 \equiv 2 \times 6 \equiv 12 \equiv 5 \pmod{7}$ (Compare to $23 \times 34 = 782 = 7 \times 111 + 5 \equiv 5 \pmod{7}$)

Example 4.8

$5^{5510} \equiv ? \pmod{7}$

$5^6 = 5^3 \times 5^3 = 125 \times 125 \equiv 6 \times 6 \equiv 36 \equiv 1 \pmod{7}$

$5^{5510} = 5^{6 \times 918 + 2} = (5^6)^{918} \times 5^2 \equiv 1^{918} \times 25 \equiv 25 \equiv 4 \pmod{7}$

Proposition 4.2 (Cancellation)

If $\gcd(c,n) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$

proof:

$n \mid ac-bc = (a-b)c$ and $\gcd(c,n) = 1 \Rightarrow n \mid a-b$ i.e. $a \equiv b \pmod{n}$ (see exercise 4.3)

Example 4.9

$4 \times 1 \equiv 4 \times 4 \pmod{6}$ but $1 \not\equiv 4 \pmod{6}$ since $\gcd(4,6) = 2 \neq 1$.

$ax \equiv b \pmod n$

Question: How to solve $ax \equiv b \pmod n$?

Proposition 4.3

$ax \equiv b \pmod n$ is solvable if and only if $\gcd(a,n) \mid b$

proof:

The equation can be solved $\Leftrightarrow$ There exists $x, q \in \mathbb{Z}$ such that $ax + nq = b$

$\Leftrightarrow \gcd(a,n) \mid b$ (see exercise 4.2)

In particular, if p is a prime, then $ax \equiv b \pmod p$ is solvable.

Also, if x_1 and x_2 are solutions of $ax \equiv b \pmod p$,

$a(x_1 - x_2) \equiv b - b \equiv 0 \pmod p$ and $\gcd(a,p) = 1$

then we have $p \mid x_1 - x_2$ (or $x_1 \equiv x_2 \pmod p$)

$\therefore$ All solutions are congruent modulo p.

Example 4.10

Solve $4x \equiv 3 \pmod 9$

Note that $\gcd(4,9) = 1$, the above equation is solvable.

$9 - 4 \times 2 = 1$ —(*) (By extended Euclidean algorithm)

$9 \times 3 + 4 \times (-2) = 3$

$4 \times (-6) \equiv 3 \pmod 9$

$\therefore -6$ is one of the solution of $4x \equiv 3 \pmod 9$

(*) shows that $4 \times (-2) \equiv 1 \pmod 9$ (or $4 \times 7 \equiv 1 \pmod 9$ if you like)

-2 acts as an "inverse" of 4

In general, $4x \equiv b \pmod 9$

$(-2)(4x) \equiv -2b \pmod 9$

$x \equiv -8x \equiv -2b \pmod 9$ (Note $-8 \equiv 1 \pmod 9$)

Another intepretation : Find $[x] \in \mathbb{Z}_9$ such that $[4][x] = [3]$

Note : $[-2][4] = [1]$ (or $[7][4] = [1]$)

We have $[4][x] = [3]$

$[-2][4][x] = [-2][3]$

$[1][x] = [-6]$

$[x] = [-6]$ (or $[3]$)

$a^m \equiv 1 \pmod n$

Question : Given $a, n \in \mathbb{Z}$, does it exist $m \in \mathbb{N}^+$ such that $a^m \equiv 1 \pmod n$?

Firstly, $a^m \equiv 1 \pmod n$ for some $m \in \mathbb{N}^+$

$\Rightarrow a \cdot a^{m-1} + nq = 1$ for some $q \in \mathbb{Z}$

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

However, if $\gcd(a,n) = 1$, does it exist $m \in \mathbb{N}^+$ such that $a^m \equiv 1 \pmod n$?

Think : There are only n elements of $\mathbb{Z}_n$, but $[a], [a^2], [a^3], \cdots \in \mathbb{Z}_n$,

so there exists $i, j \in \mathbb{N}^+$ with $i < j$ such that $[a^j] = [a^i]$ i.e $a^j \equiv a^i \pmod n$

Since $\gcd(a,n) = 1$, we can cancel a's and so $a^{j-i} \equiv 1 \pmod n$

Definition 4.6

Let $a, n \in \mathbb{Z}$ such that $\gcd(a,n) = 1$.

The order of a modulo n is the least $m \in \mathbb{N}^+$ such that $a^m \equiv 1 \pmod n$

Example 4.11

Table of a^m modulo 6

a \ m	1	2	3	4	5
0	0	0	0	0	0
1	1	1	1	1	1
2	2	4	$8 \equiv 2$	$16 \equiv 4$	$32 \equiv 2$
3	3	$9 \equiv 3$	$27 \equiv 3$	$81 \equiv 3$	$243 \equiv 3$
4	4	$16 \equiv 4$	$64 \equiv 4$	$256 \equiv 4$	$1024 \equiv 4$
5	5	$25 \equiv 1$	$125 \equiv 5$	$625 \equiv 1$	$3125 \equiv 5$

$\gcd(0,6), \gcd(2,6), \gcd(3,6), \gcd(4,6) \neq 1$

$\gcd(1,6), \gcd(5,6) = 1$

Order of $1 = 1$

Order of $5 = 2$

Definition 4.7

The Euler' φ function is defined by $\varphi(n) = |\{a \in \mathbb{N}^+ : a < n \text{ and } \gcd(a,n) = 1\}|$ for $n \in \mathbb{N}^+$

$\varphi(1) = |\{1\}| = 1$ $\qquad$ $\varphi(2) = |\{1\}| = 1$ $\qquad$ $\varphi(3) = |\{1,2\}| = 2$

$\varphi(4) = |\{1,3\}| = 2$ $\qquad$ $\varphi(5) = |\{1,2,3,4\}| = 4$ $\qquad$ $\varphi(6) = |\{1,5\}| = 2$

In particular, if p is a prime, $\varphi(p) = p-1$;

if $\gcd(p,q) = 1$, $\varphi(pq) = (p-1)(q-1)$.

(Note: $\gcd(a,pq) \neq 1$ if and only if $p|a$ or $q|a$.)

Theorem 4.6 (Euler's Theorem)

If $\gcd(a,n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Example 4.12

Table of a^m modulo 15 (with $\gcd(a,15) = 1$).

a \ m	1	2	3	4
1	1			
2	2	4	8	1
4	4	1		
7	7	4	13	1
8	8	4	2	1
11	11	1		
13	13	4	7	1
14	14	1		

Note: $\varphi(15) = 8$

Table of a^m modulo 5 (with $\gcd(a,5) = 1$)

a \ m	1	2	3	4
1	1			
2	2	4	3	1
3	3	4	2	1
4	4	1		

Note: $\varphi(5) = 4$

Idea of proof of Euler's Theorem:

1) Let $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]\in\mathbb{Z}_n : \gcd(a,n)=1\}$ $\therefore |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$

Prove that if $[a],[b]\in(\mathbb{Z}/n\mathbb{Z})^\times$, then $[a][b]=[ab]\in(\mathbb{Z}/n\mathbb{Z})^\times$.

2) Let $[a]\in(\mathbb{Z}/n\mathbb{Z})^\times$ and let $f:(\mathbb{Z}/n\mathbb{Z})^\times\longrightarrow(\mathbb{Z}/n\mathbb{Z})^\times$ defined by $f([x])=[a][x]=[ax]$.

Prove that f is bijective.

3) $\prod_{[x]\in(\mathbb{Z}/n\mathbb{Z})^\times}[x] = \prod_{[x]\in(\mathbb{Z}/n\mathbb{Z})^\times}[ax]$ (Product of all elements an $(\mathbb{Z}/n\mathbb{Z})^\times$)

$= [a^{\varphi(n)}]\prod_{[x]\in(\mathbb{Z}/n\mathbb{Z})^\times}[x]$ (Note: $[x]\in(\mathbb{Z}/n\mathbb{Z})^\times$ and by definition $\gcd(x,n)=1$, so it can be cancelled.)

$[a^{\varphi(n)}]=[1]$ i.e. $a^{\varphi(n)}\equiv 1 \pmod n$

有物不知其數，　　Let $x\in\mathbb{Z}$.

三三數之剩二，　　$x\equiv 2 \pmod 3$

五五數之剩三，　　$x\equiv 3 \pmod 5$

七七數之剩二。　　$x\equiv 2 \pmod 7$

問物幾何？　　$x=?$

孫子算經

Theorem 4.7 (Chinese Remainder Theorem)

Let $a_1,a_2,\cdots,a_k\in\mathbb{Z}$ and $n_1,n_2,\cdots,n_k\in\mathbb{N}^+$ such that $\gcd(n_i,n_j)=1$ for all $i\neq j$.

There exists $x\in\mathbb{Z}$ such that

$$x\equiv a_1 \pmod{n_1}$$
$$x\equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x\equiv a_k \pmod{n_k}$$

proof:

Let $N=n_1n_2\cdots n_k$ and $N_i=\frac{N}{n_i}=n_1\cdots n_{i-1}n_{i+1}\cdots n_k$

Note: $\gcd(n_i,n_j)=1$ for all $i\neq j$

$\Rightarrow \gcd(n_i,N_i)=1 \Rightarrow$ there exist $m_i, M_i\in\mathbb{Z}$ such that $n_im_i+N_iM_i=1 \Rightarrow N_iM_i\equiv 1 \pmod{n_i}$

Also $M_iN_i\equiv 0 \pmod{n_j}$ for $j\neq i$.

Then $x=\sum_{i=1}^{k}a_iM_iN_i$ is a solution.

Furthermore, if $x_1, x_2 \in \mathbb{Z}$ are solutions, then

$$x_1 - x_2 \equiv 0 \pmod{n_i} \quad \text{for } 1 \le i \le k.$$

$\therefore \; x_1 - x_2 \equiv 0 \pmod{N}$

$a_1 = 2, \; a_2 = 3, \; a_3 = 2, \; n_1 = 3, \; n_2 = 5, \; n_3 = 7$

$N = 3 \times 5 \times 7 = 105, \quad N_1 = 35, \; N_2 = 21, \; N_3 = 15$

$\underset{M_1}{35} \times 2 + 3 \times \underset{m_1}{(-23)} = 1 \qquad \underset{M_2}{21} \times 1 + 5 \times \underset{m_2}{(-4)} = 1 \qquad \underset{M_3}{15} \times 1 + 7 \times \underset{m_3}{(-2)} = 1$

三人同行七十稀，
五樹梅花廿一支，
七子團圓正半月，
除百零五便得知。

$x \equiv 2 \times \underset{N_1M_1}{70} + 3 \times \underset{N_2M_2}{21} + 2 \times \underset{N_3M_3}{15} \equiv 233 \equiv 23 \pmod{105}$

Example 4.13

Find $x \in \mathbb{Z}$ such that $x \equiv 3 \pmod{8}$ and $x \equiv 5 \pmod{9}$.

$n_1 = 8, \; n_2 = 9$ and so $\gcd(n_1, n_2) = \gcd(8, 9) = 1$

$a_1 = 3, \; a_2 = 5$

$N = n_1 n_2 = 8 \times 9 = 72$

$N_1 = \frac{N}{n_1} = 9 = n_2 \qquad N_2 = \frac{N}{n_2} = 8 = n_1$

$9 \times 1 + 8 \times (-1) = 1$

$N_1 M_1 + n_1 m_1 = 1$

$n_2 m_2 + N_2 M_2 = 1$

Let $x \equiv 3 \times 9 \times 1 + 5 \times 8 \times (-1) \equiv -13 \equiv 59 \pmod{72}$

$a_1 N_1 M_1 + a_2 N_2 M_2$

Exercise 4.4

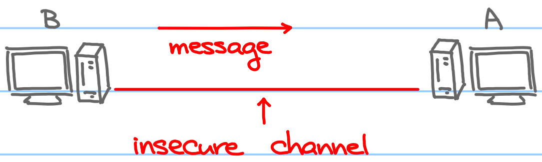
a) Find $x \in \mathbb{Z}$ such that $x \equiv 3 \pmod{7}$ and $x \equiv 13 \pmod{15}$.

Ans: $x \equiv 70 \pmod{105}$

b) Find $x \in \mathbb{Z}$ such that $x \equiv 2 \pmod{7}$, $x \equiv 3 \pmod{8}$ and $x \equiv 6 \pmod{9}$

Ans: $x \equiv 51 \pmod{504}$

RSA crytosystem



Question: How to use an insecure channel to transmit data in a secure way?

Exercise: Try to factorize 8137.

Ans: $8137 = 79 \times 103$ (Difficult?)

Idea of RSA crypstosystem: Difficult to factorize a product of two large primes!

RSA algorithm:

Key generation by A:

1) Choose two large primes p, q and compute $n = pq$.
2) Compute $\varphi(n) = \varphi(pq) = (p-1)(q-1)$ and keep private.
3) Choose $1 < e < \varphi(n)$ such that $\gcd(e, \varphi(n)) = 1$ (For example, choose a prime e and $e \nmid \varphi(n)$)
4) Find d such that $ed \equiv 1 \pmod{\varphi(n)}$ (This equation is solvable as $\gcd(e, \varphi(n)) = 1$)

   Keep d private.

Operation:

1) The pair of numbers (n, e) (called public key) is released by A.
2) Suppose $0 \le m < n$ is the message to be sent from B to A,

   B sends $c \equiv m^e \pmod{n}$ to A instead. (c is called ciphertext).
3) A computes c^d modulo n, and the result is m, i.e. $c^d \equiv m^{ed} \equiv m \pmod{n}$

Lemma 4.3

$c^d \equiv m^{ed} \equiv m \pmod n$

proof:

By Chinese remainder theorem, m is a solution of

$$(*) \begin{cases} x \equiv m \pmod p \\ x \equiv m \pmod q \end{cases}$$

therefore, for any solution x of $(*)$, we have $x \equiv m \pmod n$.

Thus, what we need to show are $m^{ed} \equiv m \pmod p$ and $m^{ed} \equiv m \pmod q$,

i.e. m^{ed} is also a solution of $(*)$, then $m^{ed} \equiv m \pmod n$.

Claim: $m^{ed} \equiv m \pmod p$

Recall: $ed \equiv 1 \pmod{\varphi(n)} \Rightarrow ed = 1 + k\varphi(n) = 1 + k(p-1)(q-1) = 1 + k\varphi(p)\varphi(q)$ for some $k \in \mathbb{Z}$.

1) If $\gcd(m,p) = 1$, then $m^{\varphi(p)} \equiv 1 \pmod p$ (Euler's theorem)

and so $m^{ed} \equiv m^{1+k\varphi(p)\varphi(q)} \equiv m \cdot (m^{\varphi(p)})^{k\varphi(q)} \equiv m \cdot 1^{k\varphi(p)} \equiv m \pmod p$

2) If $\gcd(m,p) \neq 1$, then $p \mid m$ and so $m^{ed} \equiv 0 \equiv m \pmod p$

Similarly, we can show that $m^{ed} \equiv m \pmod q$.

Example 4.14

Key generation by A:

1) Choose two primes $p = 11$, $q = 17$ and compute $n = pq = 187$

2) Compute $\varphi(n) = \varphi(pq) = (p-1)(q-1) = 10 \times 16 = 160$ and keep private.

3) Choose $1 < e < \varphi(n)$ such that $\gcd(e, \varphi(n)) = 1$ (For example, choose a prime $e = 19$)

4) Find d such that $ed \equiv 1 \pmod{\varphi(n)}$ i.e. $19d \equiv 1 \pmod{160}$

By extended Euclidean algorithm, $19 \times 59 + 160 \times (-7) = 1$, i.e. $19 \times 59 \equiv 1 \pmod{160}$ (↑ e, ↑ d, ↑ $\varphi(n)$)

Keep $d = 59$ private.

Operation:

1) Public key $(n, e) = (187, 19)$ is released by A.

2) Suppose $0 \le m = 32 < 187$ is the message to be sent from B to A,

B sends the ciphertext $c \equiv m^e \equiv 32^{19} \equiv 43 \pmod{n = 187}$ to A instead.

3) A computes $m \equiv c^d \equiv 43^{59} \equiv 32 \pmod{n = 187}$

Exercise 4.5

Find c if we use $m = 53$ (Ans: $c = 93$), verify your answer by computing c^d modulo n.