Chapter 4 (Part 1)

數論介紹

Introduction to Number Theory

Definition 4. 1

Every integer is either even or odd, but not both. An integer n is said to be

(a) *even* if $n = 2k$ for some integer k, and
(b) *odd* if $n = 2k + 1$ for some integer k.

EXAMPLE 4. 1

Show that, for every pair of odd integers, the product is odd.

Proof :

Let m and n be arbitrary odd integers.
So $m = 2k + 1$ and $n = 2l + 1$ for some $k, l \in \mathbf{Z}$
Hence,

$$mn = (2k+1)(2l+1) = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1.$$

Since $2kl + k + l$ is an integer, the form displayed on

the right-hand side above shows that mn is odd.

EXAMPLE 4. 2

Let $n \in \mathbf{Z}$. Show: If n^2 is odd, then n is odd.

Hint: prove by its contrapositive statement.

Proof :

Suppose n is not odd.
That is, n is even.
So $n = 2k$ for some $k \in \mathbf{Z}$.
Hence, $n^2 = 4k^2 = 2(2k^2)$.
Since $2k^2 \in \mathbf{Z}$, n^2 is even.
That is, n^2 is not odd.

EXAMPLE 4.3

Similarly, let $n \in \mathbf{Z}$. Show: If n^2 is even, then n is even.

Hint: prove by its contrapositive statement.

Proof :

Since m is an odd number, $m = 2h + 1$ for some $h \in \mathbf{Z}$.

So $m^2 = (2h + 1)^2$

$= 4h^2 + 4h + 1 = 2(2h^2 + 2h) + 1$

Because $(2h^2 + 2h) \in \mathbf{Z}$.

So m^2 is an odd number.

Definition 4. 2

Given integers a and b, $b \neq 0$, we say that b *divides* a, written $b \mid a$, if $a = bn$ for some integer n.

In this case, we also say that a is *divisible* by b, that a is a *multiple* of b, that b is a *divisor* of a, and that b is a *factor* of a.

When a is not divisible by b, we write $b \nmid a$.

若 a，$b \in \mathbf{Z}$ 且 $b \neq 0$，我們稱 b **整除** (divides) a，且記 $b|a$，若存在整數 n 使得 $a = bn$。當這個發生，我們稱 b 是 a 的**因數** (divisor)，或 a 是 b 的**倍數** (multiple)。

EXAMPLE 4.4

Let a, b, and c be integers. Show: If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof :

Suppose $a \mid b$ and $b \mid c$.
So $b = ak$ and $c = bl$ for some $k, l \in \mathbf{Z}$.
Observe that $c = bl = akl = a(kl)$.
Since $kl \in \mathbf{Z}$, we have established that $a \mid c$.

THEOREM 4.1

For all $a, b, c \in \mathbf{Z}$

a) $1|a$ and $a|0$.

b) $[(a|b) \wedge (b|a)] \Rightarrow a = \pm b$.

c) $[(a|b) \wedge (b|c)] \Rightarrow a|c$.

d) $a|b \Rightarrow a|bx$ for all $x \in \mathbf{Z}$.

e) If $x = y + z$, for some $x, y, z \in \mathbf{Z}$, and a divides two of the three integers x, y, and z, then a divides the remaining integer.

f) $[(a|b) \wedge (a|c)] \Rightarrow a|(bx + cy)$, for all $x, y \in \mathbf{Z}$.
(The expression $bx + cy$ is called a *linear combination of* b, c.)
線性組合

Proof : (c) Same as Example 4.4
(d) Exercise

THEOREM 4.1 Cont.

For all a, b, $c \in \mathbf{Z}$

a) $1|a$ and $a|0$.

b) $[(a|b) \wedge (b|a)] \Rightarrow a = \pm b$.

Proof :

THEOREM 4.1 Cont.

For all $a, b, c \in \mathbf{Z}$

e) If $x = y + z$, for some $x, y, z \in \mathbf{Z}$, and a divides two of the three integers x, y, and z, then a divides the remaining integer.

Proof :

THEOREM 4.1 Cont.

For all $a, b, c \in \mathbf{Z}$

f) $[(a|b) \wedge (a|c)] \Rightarrow a|(bx + cy)$, for all $x, y \in \mathbf{Z}$.

Proof :

If $a|b$ and $a|c$, then $b = am$ and $c = an$, for some $m, n \in \mathbf{Z}$.

So $bx + cy = (am)x + (an)y = a(mx + ny)$

Since $bx + cy = a(mx + ny)$, with $mx + ny \in \mathbf{Z}$,

it follows that $a|(bx + cy)$.

EXAMPLE 4.5

Let $a, b \in \mathbf{Z}$ so that $2a + 3b$ is a multiple of 17. (For example, we could have $a = 7$ and $b = 1$ — and $a = 4$, $b = 3$ also works.)

Prove that 17 divides $9a + 5b$.

Proof:

We observe that $17|(2a + 3b) \Rightarrow 17|(-4)(2a + 3b)$, by **Thm. 4.1(d)**.

Also, since $17|17$, it follows from **Thm. 4.1(d)** that $17|(17a + 17b)$.

Hence, $17|[(17a + 17b) + (-4)(2a + 3b)]$, by part **Thm. 4.1(e)**.

Consequently, as $[(17a + 17b) + (-4)(2a + 3b)]$
$= [(17 - 8)a + (17 - 12)b] = 9a + 5b$, we have $17|(9a + 5b)$.

THEOREM 4.2

Let $a, b \in \mathbf{Z}$ with $b > 0$. If $a \mid b$, then $a \leq b$.

Proof:

Suppose $a \mid b$.
So $b = ak$ for some $k \in \mathbf{Z}$.

Case 1: $a \leq 0$.
We have $a \leq 0 < b$, and the conclusion $a \leq b$ is immediate.

Case 2: $a > 0$.
Since $ak = b > 0$, it must be that $k > 0$ too. (Otherwise, $ak < 0$.)
Since k is an integer, $1 \leq k$.
Multiplication by (the positive value) a gives that

$$a = a \cdot 1 \leq a \cdot k = b.$$

In both cases, we conclude that $a \leq b$.

Definition 4. 3

An integer p is said to be *prime* (質數) if $p > 1$ and the only positive divisors of p are 1 and p.

An integer $n > 1$ that is not prime is said to be *composite* (合成數).

The first ten primes are: 2, 3, 5, 7, 11, 13, 17, 19, 23, and 29.

The first ten composites are:

$4 = 2 \cdot 2,\quad 9 = 3 \cdot 3,\quad 14 = 2 \cdot 7,\quad 18 = 3 \cdot 6.$

$6 = 2 \cdot 3,\quad 10 = 2 \cdot 5,\quad 15 = 3 \cdot 5,$

$8 = 2 \cdot 4,\quad 12 = 2 \cdot 6,\quad 16 = 2 \cdot 8,$

Definition 4. 4

An integer c is said to be a *common divisor* of the integers m and n if

$$c \mid m \text{ and } c \mid n.$$

Definition 4. 5

Given integers m and n not both zero, their *greatest common divisor*, denoted $\gcd(m, n)$, is the unique integer d such that

(i) $d > 0$,

(ii) $d \mid m$ and $d \mid n$, and

(iii) $\forall\, c \in \mathbf{Z}^+$, if $c \mid m$ and $c \mid n$, then $c \leq d$.

Definition 4. 6

Given nonzero integers a and b, their *least common multiple*, denoted $\mathrm{lcm}(a, b)$, is the unique integer m such that

(i) $m > 0$,

(ii) $a \mid m$ and $b \mid m$, and

(iii) $\forall\, n \in \mathbf{Z}^+$, if $a \mid n$ and $b \mid n$, then $m \le n$.

Definition 4.7

Two integers m and n are said to be *relatively prime* if $\gcd(m, n) = 1$.

EXAMPLE 4.6

(1) $\gcd(18, 30) = 6$.

Certainly, $6 > 0$, $6 \mid 18$, and $6 \mid 30$. Also, any element c in the set $\{1, 2, 3, 6\}$ of positive common divisors of 18 and 30 satisfies $c \leq 6$.

(2) Observe that 14 and 9 are relatively prime, since $\gcd(14, 9) = 1$.

EXAMPLE 4.7

Given any positive integer k, show: $\gcd(k, 0) = k$.

Proof:

Observe that k is positive and that $k \mid k$ and $k \mid 0$.

Hence, conditions (i) and (ii) are satisfied.

If $c \in \mathbf{Z}^+$ and $c \mid k$ and $c \mid 0$, then, by Theorem 4.2, we have $c \leq k$. Thus, condition (iii) is satisfied.

We conclude that $k = \gcd(k, 0)$.

EXAMPLE 4.8

Prove that $\sqrt{2}$ is irrational.

Hint: proof by contradiction

Proof :

Suppose $\sqrt{2}$ was rational.

Choose m, n integers without common prime factors (always possible) such that $\sqrt{2} = \dfrac{m}{n}$

Show that m and n are both even,

thus having a common factor 2, a **contradiction**!

Want to prove both m and n are even.

$$\sqrt{2} = \frac{m}{n}$$

$$\sqrt{2}n = m$$

$$2n^2 = m^2$$

so m is even.

so can assume $m = 2l$ $l \in \mathbf{Z}$

$$m^2 = 4l^2$$

$$2n^2 = 4l^2$$

$$n^2 = 2l^2$$

so n is even.

Well-Ordering Principle 良序原理

Well-Ordering Principle for the Integers

Each nonempty subset of the nonnegative/positive integers has a smallest element.

$\{0, 1, 2, 3, \ldots\}$
$\{1, 2, 3, \ldots\}$

THEOREM 4.3

If $n \in \mathbf{Z}^+$ and n is composite, then there is a prime p such that $p|n$.

Proof:

If not, let S be the set of all composite integers that have no prime divisors. If S is not empty, then by the well-ordering principle, S has a least element m. But if m is composite, then $m = m_1 m_2$ with $1 < m_1 < m$ and $1 < m_2 < m$.

Since m_1 is not in S, m_1 is a prime or divisible by a prime, which means m is also divisible by a prime. This leads to a contradiction, and thus $S = \varnothing$.

If $n \in \mathbf{Z}^+$ and n is composite, then there is a prime p such that $p|n$.

Proof by contradiction:

If not,

let $S = \{\, n \mid n \in \mathbf{Z}^+ \wedge (n \text{ is composite}) \wedge (n \text{ has no prime divisors})\}$.

$\boxed{S \neq \varnothing} \Rightarrow \boxed{\exists m \in S,\ s.t.\ \forall n \in S,\ m \leq n}$ (by the well-ordering principle).

$\boxed{m \text{ is composite}} \Rightarrow \boxed{m = m_1 m_2, \quad \text{where } 1 < m_1 < m \text{ and } 1 < m_2 < m.}$

$\boxed{m_1 \notin S} \Rightarrow \boxed{(m_1 \text{ is a prime}) \vee (m_1 \text{ is divisible by a prime})}$

$\Rightarrow \boxed{(m \text{ is also divisible by a prime})}$

Contradiction!!!

Thus $S = \varnothing$.

THEOREM 4.4

(歐幾里得) 有無限多個質數。

(Euclid) There are infinitely many primes.

Proof: If not, let $p_1, p_2, \cdots, p_k$ be the finite set of primes, and let $B = p_1 p_2 \cdots p_k + 1$. Since $B > p_i$ for all $1 \le i \le k$, B cannot be a prime. Hence B is a composite. So by **Theorem 4.3** there is a prime p_j and $p_j \mid B$. Since $p_j \mid B$ and $p_j \mid p_1 p_2 \cdots p_k$, it follows that $p_j \mid 1$, a contradiction.

(Note: by **Theorem 4.1**(e).)

(Note: by **Theorem 4.2**, $p_j \le 1$, but the smallest prime is 2.)

Division Algorithm

Given any integer n and any positive integer d, there exist unique integers q and r such that $n = dq + r$ and $0 \leq r < d$.

Definition 4. 8

n: *dividend* （被除數）

d: *divisor* （除數）

q: *quotient* （商數）

r: *remainder* （餘數）

We also write

$$q = n \; div \; d \quad \text{and} \quad r = n \bmod d$$

EXAMPLE 4.9

(1) If $a = 124$ and $b = 9$, then $q = 13$ and $r = 7$.

That is, $124 = 9(13) + 7$.

So $124 \text{ div } 9 = 13$ and $124 \bmod 9 = 7$.

(2) If $a = 60$ and $b = 5$, then $q = 12$ and $r = 0$.

That is, $60 = 5(12) + 0$.

So $60 \text{ div } 5 = 12$ and $60 \bmod 5 = 0$.

Definition 4. 9

Given integers a, b, and n with $n > 1$, we say that a is *congruent* (同餘) to b *modulo* n, written

$$a \equiv b \pmod{n},$$

if $n \mid (a - b)$.

EXAMPLE 4.10

(Some Congruences)

$14 \equiv 2 \pmod{12}$, since $12 \mid (14 - 2)$

$-4 \equiv 8 \pmod{12}$, since $12 \mid (-4 - 8)$

$34 \equiv 6 \pmod{7}$, since

$25 \equiv 0 \pmod{5}$, since

THEOREM 4.5

Arithmetic Properties of Congruence

Let a_1, a_2, b_1, b_2, and n be integers with $n > 1$. If $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then

(a) $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$, *and*

(b) $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.

Proof: **(b)** Suppose $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$.

Therefore, $n \mid (a_1 - a_2)$ and $n \mid (b_1 - b_2)$.

That is, $a_1 - a_2 = nk$ and $b_1 - b_2 = nl$ for some $k, l \in \mathbf{Z}$.

Observe that
$$\begin{aligned} a_1 b_1 - a_2 b_2 &= a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2 \\ &= a_1(b_1 - b_2) + b_2(a_1 - a_2) \\ &= a_1 nl + b_2 nk = n\underbrace{(a_1 l - b_2 k)}_{\in \mathbf{Z}}. \end{aligned}$$

Therefore, $n \mid (a_1 b_1 - a_2 b_2)$,
and it follows that $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.

EXAMPLE 4.11

Note that $4 \equiv -6 \pmod{10}$ and $22 \equiv 2 \pmod{10}$.
As promised by Theorem 4.5,

$$4 + 22 \equiv -6 + 2 \pmod{10}$$

and

$$4 \cdot 22 \equiv -6 \cdot 2 \pmod{10}.$$

COROLLARY 4.6

Let m, a_1, a_2, and n be integers with $n > 1$. If $a_1 \equiv a_2 \pmod{n}$, then

(a) $ma_1 \equiv ma_2 \pmod{n}$, *and*

(b) *if $m \geq 0$, then $a_1^m \equiv a_2^m \pmod{n}$.*

EXAMPLE 4.12

Note that $3 \equiv -2 \pmod{5}$.

As promised by Corollary 4.6, we also have

$$4(3) \equiv 4(-2) \pmod{5}$$

and

EXAMPLE 4.13

Use Theorems to help with the following calculations.

(1) Compute $(5162387 + 83645) \bmod 10$.

Since $5162387 \equiv 7 \pmod{10}$ and

$83645 \equiv 5 \pmod{10}$,

by Theorem 4.5,

we get $5162387 + 83645 \equiv 5 + 7 \pmod{10}$.

$\equiv 12 \pmod{10}$.

$\equiv 2 \pmod{10}$.

EXAMPLE 4.13 Cont.

(2) Compute 2^{23} mod 5.

Note that $2^4 = 16 \equiv 1\ (mod\ 5)$

By Corollary 4.6,

$$2^{20} = (2^4)^5 \equiv 1^5 \equiv 1\ (mod\ 5)$$

By Corollary 4.6,

$$2^{23} = 2^{20} \cdot 2^3 \equiv 2^{20} \cdot 8 \equiv 1 \cdot 8 \equiv 8 \equiv 3\ (mod\ 5)$$

Therefore,

Euclid's Algorithm

Let x_1 and x_2 be two positive integers and we want to obtain gcd(x_1, x_2).

e.g.

$$x_1 > x_2 \qquad\qquad 338 > 117$$

$$x_1 = q_1 x_2 + x_3$$

$$x_2 = q_2 x_3 + x_4$$

$$\vdots$$

$$x_{n\text{-}2} = q_{n\text{-}2} x_{n\text{-}1} + x_n$$

$$x_{n\text{-}1} = q_{n\text{-}1} x_n + 0$$

$$\gcd(x_1, x_2) = x_n$$

$$338 = 2 * 117 + 104$$

$$117 = 1 * 104 + 13$$

$$104 = 8 * 13 + 0$$

$$\gcd(338, 117) = 13$$

Euclid's Algorithm

Let x_1 and x_2 be two positive integers and we want to obtain $\gcd(x_1, x_2)$.

e.g.

$$\begin{array}{rl} & x_1 > x_2 \\ x_1 & \bmod x_2 = x_3 \\ x_2 & \bmod x_3 = x_4 \\ & \cdots \\ x_{n-1} & \bmod x_n = 0 \end{array} \qquad \begin{array}{rl} & 338 > 117 \\ 338 & \bmod 117 = 104 \\ 117 & \bmod 104 = 13 \\ & \\ 104 & \bmod 13 = 0 \end{array}$$

The final number before reach 0 will always be the greatest common divisor.

$$\gcd(x_1, x_2) = x_n \qquad \gcd(338, 117) = 13$$

THEOREM 4. 7

Bézout's identity

$$\forall\ a, b \in \mathbf{Z}^*, \exists\ u, v \in \mathbf{Z} \text{ such that } \gcd(a, b) = ua + vb$$

Proof: Let $a = x_1$ and $b = x_2$, suppose $a > b$

Euclid's Algorithm

$$x_1 = q_1 x_2 + x_3$$
$$x_2 = q_2 x_3 + x_4$$
$$\vdots$$
$$x_{n-2} = q_{n-2} x_{n-1} + x_n$$
$$x_{n-1} = q_{n-1} x_n + 0$$

Inversing Euclid's Algorithm

$$x_n = x_{n-2} - q_{n-2} x_{n-1}$$
$$x_{n-1} = x_{n-3} - q_{n-3} x_{n-2}$$
$$\vdots$$
$$x_4 = x_2 - q_2 x_3$$
$$x_3 = x_1 - q_1 x_2$$

THEOREM 4. 7

Bézout's identity

$$\forall\ a\ ,\ b \in \mathbf{Z}^*, \exists\ u,\ v \in \mathbf{Z} \text{ such that } \gcd(a, b) = ua + vb$$

Proof: Let $a = x_1$ and $b = x_2$, suppose $a > b$

Euclid's Algorithm

$$x_1 = q_1 x_2 + x_3$$
$$x_2 = q_2 x_3 + x_4$$
$$\vdots$$
$$x_{n\text{-}2} = q_{n\text{-}2} x_{n\text{-}1} + x_n$$
$$x_{n\text{-}1} = q_{n\text{-}1} x_n + 0$$

Inversing Euclid's Algorithm

$$x_n = x_{n\text{-}2} - q_{n\text{-}2} x_{n\text{-}1}$$
$$x_{n\text{-}1} = x_{n\text{-}3} - q_{n\text{-}3} x_{n\text{-}2}$$
$$\vdots$$
$$x_4 = x_2 - q_2 x_3$$
$$x_3 = x_1 - q_1 x_2$$

$$\gcd(x_1, x_2) = x_n \qquad x_n = u\, x_1 + v\, x_2$$

EXAMPLE 4.14

Example: $\gcd(252,198) = 18$

Using the divisions performed by the Euclid Algorithm:

$$252 = 1\times 198 + 54 \quad \text{----------------} \; (1)$$
$$198 = 3 \times 54 + 36 \quad \text{----------------} \; (2)$$
$$54 = 1 \times 36 + 18 \quad \text{----------------} \; (3)$$
$$36 = 2 \times 18$$

So, $18 = 54 - 1 \times 36$ (from 3) and

$36 = 198 - 3 \times 54$ (from 2)

Therefore $18 = 54 - 1 \times (198 - 3 \times 54) = 4 \times 54 - 1 \times 198$

But (from 1) $54 = 252 - 1\times 198$;

We get $18 = 4\,(252 - 1\times 198) - 1 \times 198 = \mathbf{4} \times 252 \mathbf{-} \mathbf{5} \times 198$

THEOREM 4.8

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

Proof:

Since $ac \equiv bc \pmod{n}$ this means $n \mid ac - bc$.
Factoring the right side, we get $n \mid c(a - b)$.

Since $\gcd(c, n) = 1$ (c and n are relative prime),
by Bezout's Identity Theorem, $\exists u, v$ s.t. $uc + vn = 1$.
So, $uc\,(a - b) + vn\,(a - b) = (a - b)$.

We have, $n \mid c(a - b)$, thus $n \mid uc(a - b)$, and also $n \mid vn\,(a - b)$.
This implies that $n \mid a - b$, in other words, $a \equiv b \pmod{n}$.

EXAMPLE 4.15

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

$$24 \equiv 15 \pmod{9}$$

$$8 * 3 \equiv 5 * 3 \pmod{9}$$

$$8 \not\equiv 5 \pmod{9}$$

$$60 \equiv 15 \pmod{9}$$

$$12 * 5 \equiv 3 * 5 \pmod{9}$$

$$12 \equiv 3 \pmod{9}$$

Definition 4. 10

A congruence of the form

$$ax \equiv b \pmod{n}$$

where n is a positive integer, a, b are integers and x is an integer variable is called a linear congruence.

Definition 4. 11

An integer a' such that $a' a \equiv 1 \pmod{n}$ is called a multiplicative inverse of a modulo n.

EXAMPLE 4.16

(1) Find a multiplicative inverse of 4 modulo 9.

(2) Find a multiplicative inverse of 5 modulo 15.

(1)

$1*4 = 4 \equiv -5 \pmod 9$,
$2*4 = 8 \equiv -1 \pmod 9$,
$3*4 = 12 \equiv 3 \pmod 9$,
$4*4 = 16 \equiv 7 \pmod 9$,
$5*4 = 20 \equiv 2 \pmod 9$,
$6*4 = 24 \equiv 6 \pmod 9$,
$7*4 = 28 \equiv 1 \pmod 9$,
$8*4 = 32 \equiv 5 \pmod 9$,
$9*4 = 36 \equiv 0 \pmod 9$,
$10*4 = 40 \equiv 4 \pmod 9$,

Thus, 7 is a multiplicative inverse of 4 modulo 9.

(2) Where is the inverse?

THEOREM 4. 9

If gcd(a, n) = 1 and n >1, then a has a unique (modulo n) inverse a'.

Proof:

By Bezout's Identity Theorem, $\exists u,v$ s.t. $ua + vn = 1$,

so $ua + vn \equiv 1 \pmod{n}$.

Since $vn \equiv 0 \pmod{n}$, $ua \equiv 1 \pmod{n}$.

Thus u is an inverse of a (mod n). (i.e., $a' = u$)

Theorem 4.8 guarantees that if $ua \equiv wa \equiv 1$ then $u \equiv w \pmod{n}$.

Thus this inverse is **unique** mod n .

(Theorem 4.8 : If $ac \equiv bc \pmod{n}$ and gcd(c, n) = 1, then $a \equiv b \pmod{n}$.)

EXAMPLE 4.17

What are the solutions of the linear congruence $4x \equiv 5 \pmod 9$?

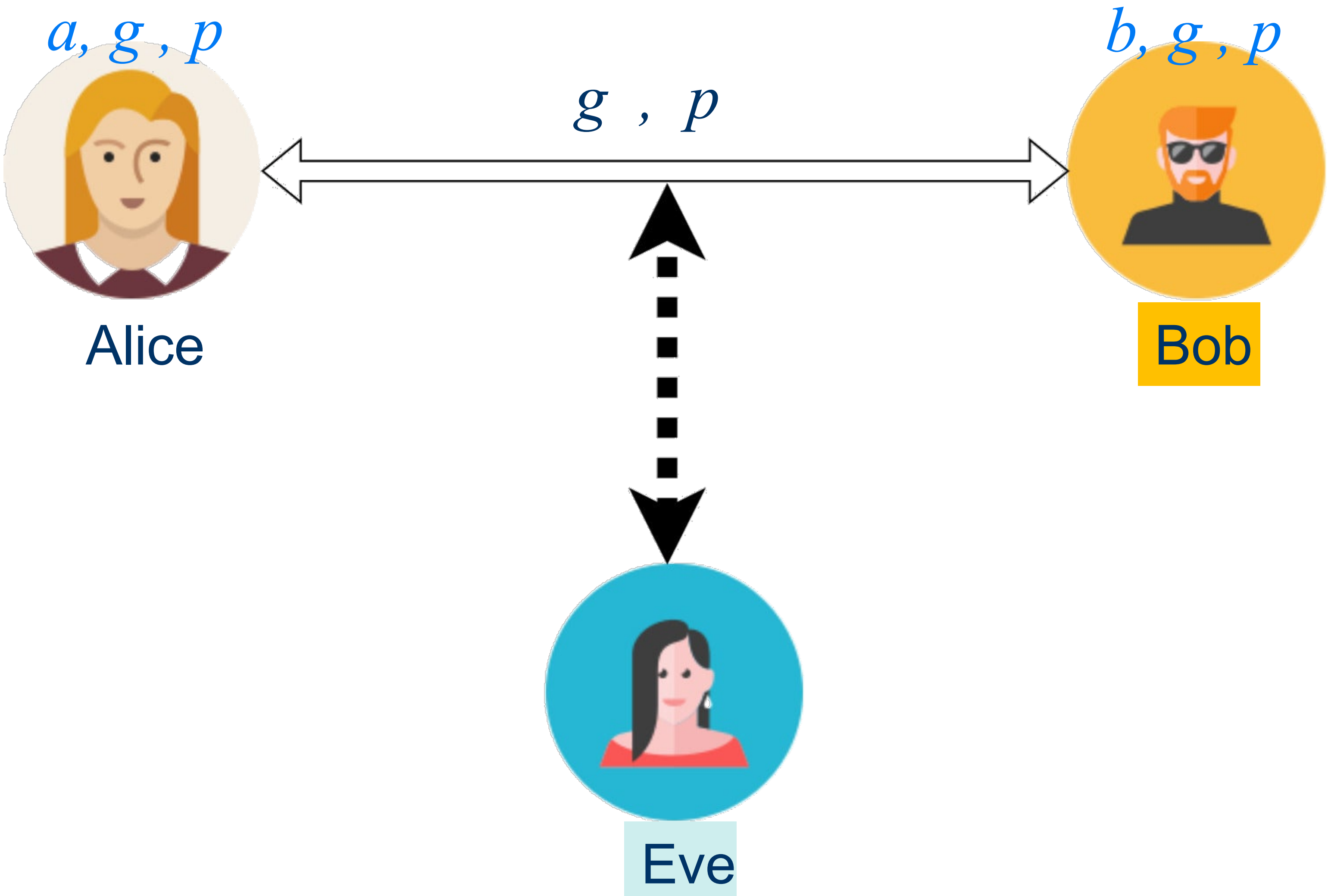
Since we know that 7 is an inverse for 4 mod 9, we can multiply both sides of the linear congruence:

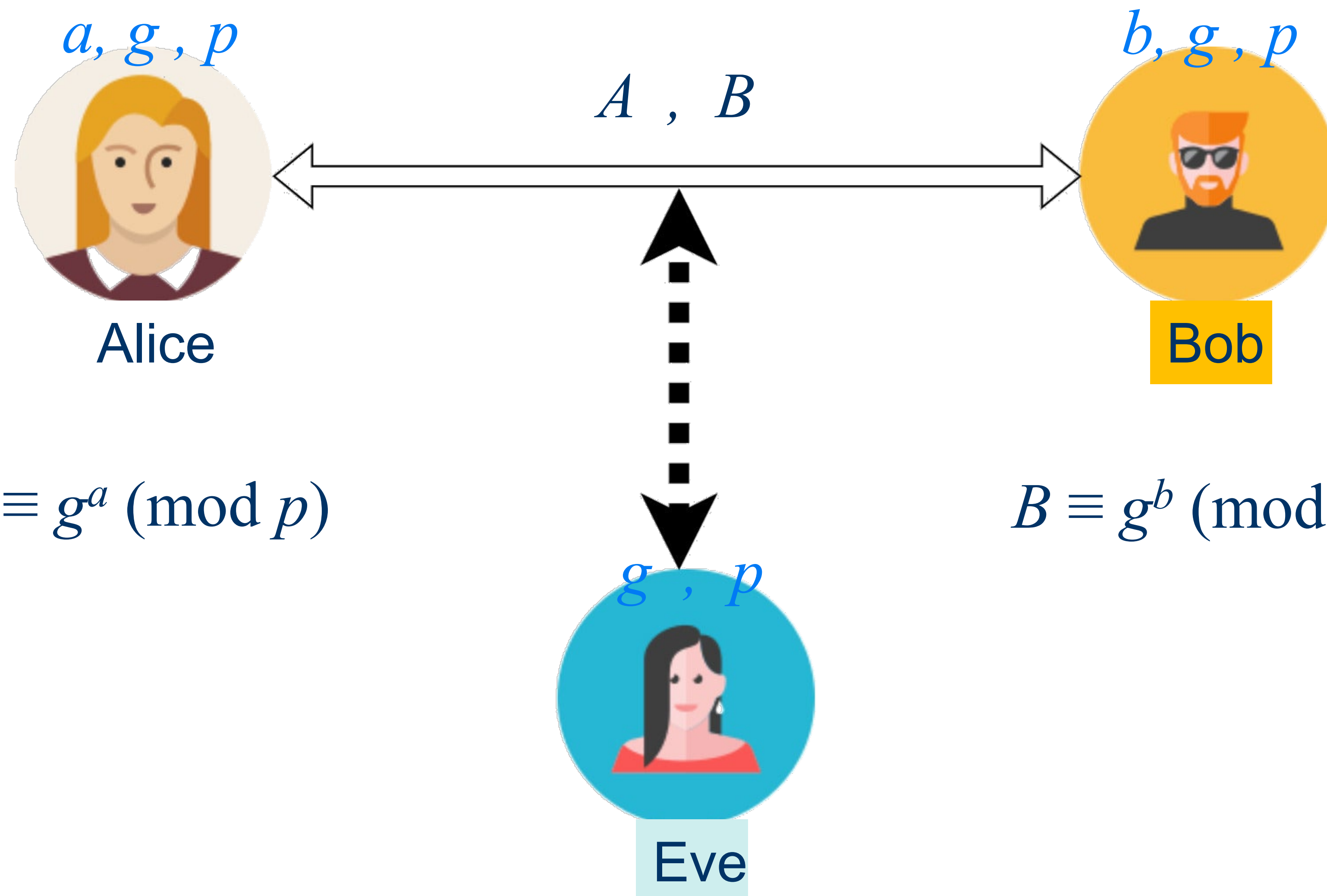
$$7 \times 4x \equiv 7 \times 5 \pmod 9$$

Since $28 \equiv 1 \pmod 9$ and $35 \equiv 8 \pmod 9$, it follows that if x is a solution, then $x \equiv 8 \pmod 9$.

So, solutions are, 8, 17, 26, …, and -1, -10, etc.

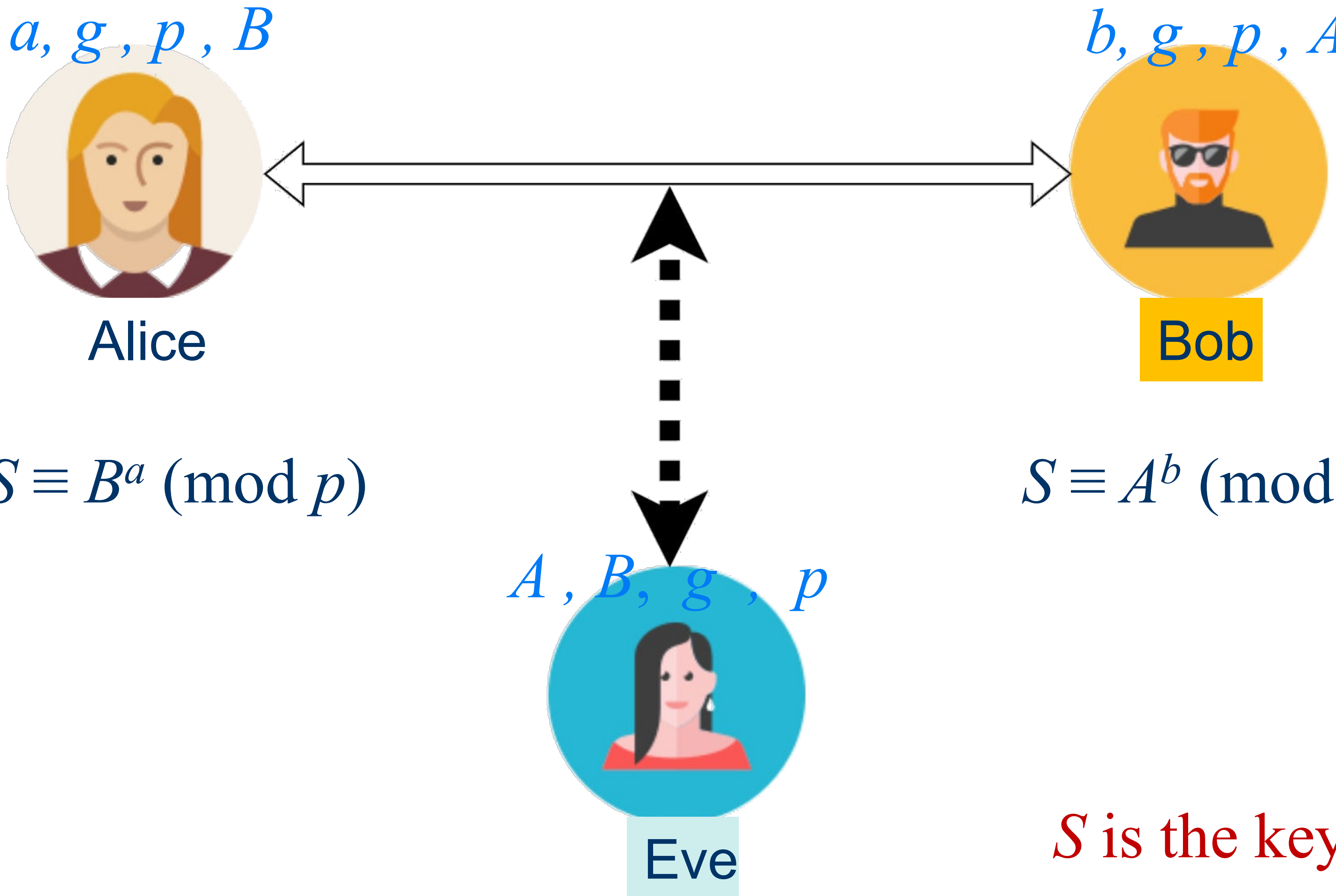
Diffie-Hellman Key Exchange





$A \equiv g^a \pmod{p}$

$B \equiv g^b \pmod{p}$

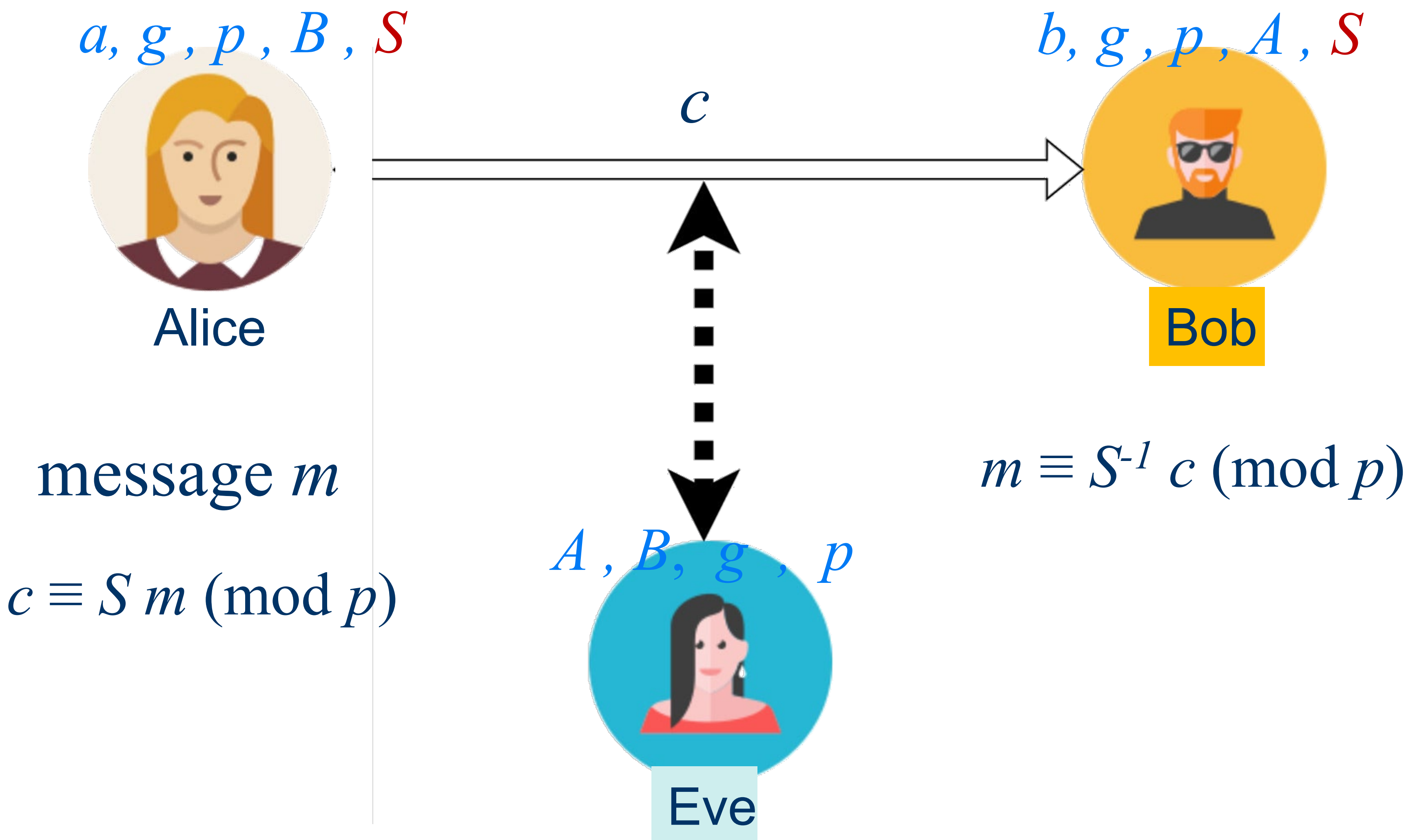


$S \equiv B^a \pmod{p}$

$S \equiv A^b \pmod{p}$

S is the key

$$S \equiv B^a \pmod{p} \equiv g^{ba} \pmod{p} \equiv g^{ab}\ (\mathrm{mod\ p}) \equiv \boxed{}$$



Eve may still be able to calculate a or b by a powerful computer. In order to prevent this, Alice and Bob need to choose very large p, g, a and b.

EXAMPLE 4.18

Suppose $g = 7,\ p = 659,\ a = 442,$

calculate $A \equiv g^a \pmod{p}$

$7^2 \equiv 49 \pmod{659}$

$7^4 \equiv 49 \times 49 \equiv 424 \pmod{659}$

$7^8 \equiv 424 \times 424 \equiv 528 \pmod{659}$

$7^{16} \equiv 528 \times 528 \equiv 27 \pmod{659}$

$7^{32} \equiv 27 \times 27 \equiv 70 \pmod{659}$

$7^{64} \equiv 70 \times 70 \equiv 287 \pmod{659}$

$7^{128} \equiv 287 \times 287 \equiv 653 \pmod{659}$

$7^{256} \equiv 653 \times 653 \equiv 36 \pmod{659}$

$$7^{442} = 7^{256+128+32+16+8+2} \equiv 36 \times 653 \times 70 \times 27 \times 528 \times 49 \pmod{659}$$

$$\equiv \boxed{}$$

EXAMPLE 4.19

Finding S^{-1}, which is the inverse of S modulo p.

Suppose $S = 720$ and $p = 1777$

Euclid's Algorithm

$1777 \bmod 720 = 337 \quad \Rightarrow \quad 1777 - 2 \times 720 = 337$

$720 \bmod 337 = 46 \quad \Rightarrow \quad 720 - 2 \times 337 = 46$

$337 \bmod 46 = 15 \quad \Rightarrow \quad 337 - 7 \times 46 = 15$

$46 \bmod 15 = 1 \quad \Rightarrow \quad 46 - 3 \times 15 = 1$

Goal:

$$u \times 720 + v \times 1777 = 1$$

$$u \times 720 + v \times 1777 \equiv 1 \pmod{1777}$$

$$u \times 720 \equiv 1 \pmod{1777}$$

EXAMPLE 4.19 Cont.

Euclid's Algorithm

$$1777 \bmod 720 = 337 \quad \Rightarrow \quad 1777 - 2 \times 720 = 337$$

$$720 \bmod 337 = 46 \quad \Rightarrow \quad 720 - 2 \times 337 = 46$$

$$337 \bmod 46 = 15 \quad \Rightarrow \quad 337 - 7 \times 46 = 15$$

$$46 \bmod 15 = 1 \quad \Rightarrow \quad 46 - 3 \times 15 = 1$$

$$720 - 2 \times 337 = 46 \quad \Rightarrow \quad 720 - 2 \times (1777 - 2 \times 720) = 46 \quad \Rightarrow \quad 5 \times 720 - 2 \times 1777 = 46$$

$$337 - 7 \times 46 = 15 \quad \Rightarrow \quad (1777 - 2 \times 720) - 7 \times (5 \times 720 - 2 \times 1777) = 15$$

$$\Rightarrow 15 \times 1777 - 37 \times 720 = 15$$

$$46 - 3 \times 15 = 1 \quad \Rightarrow \quad (5 \times 720 - 2 \times 1777) - 3 \times (15 \times 1777 - 37 \times 720) = 1$$

$$\Rightarrow \quad 116 \times 720 - 47 \times 1777 = 1$$

$$\Rightarrow \quad 116 \times 720 \bmod 1777 = 1$$