Lecture 6. Number Theory

DR. YARASLAU ZADVORNY

Division with remainder

Suppose a is an integer and b is a positive integer. Then there exist unique integers q and r such that $0 \leq r < b$ and

$$a = bq + r.$$

In the last equality, a is called the dividend, b is called the divisor, q is called the quotient and r is called the remainder.

Division with remainder

Suppose a is an integer and b is a positive integer. Then there exist unique integers q and r such that $0 \leq r < b$ and

$$a = bq + r.$$

In the last equality, a is called the dividend, b is called the divisor, q is called the quotient and r is called the remainder.

Examples: $a = 32$, $b = 5$. Then $32 = 5 \times 6 + \mathbf{2}$

- $a = -44$, $b = 8$. Then $-44 = 8 \times (-6) + \mathbf{4}$

Congruence

Let a and b be integers and m be a positive integer. We say that a is congruent to b modulo m if the remainders of the numbers a and b modulo m are equal. If it is so, we write

$$a \equiv b \pmod{m}.$$

Congruence

Let a and b be integers and m be a positive integer. We say that a is congruent to b modulo m if the remainders of the numbers a and b modulo m are equal. If it is so, we write

$$a \equiv b \pmod{m}.$$

Note that in fact $a \equiv b \pmod{m}$ if and only if a – b is divisible by m. Indeed, if $a = mp + r$ and $b = mq + r$ then $a – b = m(p – q)$.

Congruence

Let a and b be integers and m be a positive integer. We say that a is congruent to b modulo m if the remainders of the numbers a and b modulo m are equal. If it is so, we write

$$a \equiv b \pmod{m}.$$

Note that in fact $a \equiv b \pmod{m}$ if and only if a – b is divisible by m. Indeed, if $a = mp + r$ and $b = mq + r$ then $a - b = m(p - q)$.

In particular, if $a = mp + r$ then $a - r$ is divisible by m $a \equiv r \pmod{m}$. Often, when we write that, say, $23 \equiv 2 \pmod{7}$ we simply mean that 23 gives remainder 2 modulo 7.

Properties

1) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$.

Properties

1) If $a \equiv b$ (mod m) and $c \equiv d$ (mod m) then $a + c \equiv b + d$ (mod m).

Proof. If $a - b \vdots m$ and $c - d \vdots m$ then $(a - b) + (c - d) \vdots m$.

Properties

1) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$.

Proof. If $a - b \vdots m$ and $c - d \vdots m$ then $(a - b) + (c - d) \vdots m$.

2) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$.

Properties

1) If $a \equiv b$ (mod m) and $c \equiv d$ (mod m) then $a + c \equiv b + d$ (mod m).

Proof. If $a - b \vdots m$ and $c - d \vdots m$ then $(a - b) + (c - d) \vdots m.$

2) If $a \equiv b$ (mod m) and $c \equiv d$ (mod m) then $ac \equiv bd$ (mod m).

Proof. If $a - b \vdots m$ and $c - d \vdots m$ then

$$ac - bd = ac - ad + ad - bd = a(c - d) + d(a - b) \vdots m.$$

Properties

1) If $a \equiv b$ (mod m) and $c \equiv d$ (mod m) then $a + c \equiv b + d$ (mod m).

Proof. If $a - b \vdots m$ and $c - d \vdots m$ then $(a - b) + (c - d) \vdots m.$

2) If $a \equiv b$ (mod m) and $c \equiv d$ (mod m) then $ac \equiv bd$ (mod m).

Proof. If $a - b \vdots m$ and $c - d \vdots m$ then

$$ac - bd = ac - ad + ad - bd = a(c - d) + d(a - b) \vdots m.$$

3) If $a \equiv b$ (mod m) then $a^n \equiv b^n$ (mod m).

Properties

1) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$.

Proof. If $a - b \vdots m$ and $c - d \vdots m$ then $(a - b) + (c - d) \vdots m$.

2) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$.

Proof. If $a - b \vdots m$ and $c - d \vdots m$ then

$$ac - bd = ac - ad + ad - bd = a(c - d) + d(a - b) \vdots m.$$

3) If $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$.

Proof. According to the property 2), if $a \equiv b \pmod{m}$ then $a \times a \equiv b \times b \pmod{m}$, or $a^2 \equiv b^2 \pmod{m}$; again, according to property 2), if $a \equiv b \pmod{m}$ and $a^2 \equiv b^2 \pmod{m}$, then $a^2 \times a \equiv b^2 \times b \pmod{m}$, or $a^3 \equiv b^3 \pmod{m}$, etc.

Properties (what about the division?)

4) If $ka \equiv kb \pmod{m}$ and $\gcd(k, m) = 1$ then $a \equiv b \pmod{m}$.

Properties (what about the division?)

4) If $ka \equiv kb \pmod{m}$ and $\gcd(k, m) = 1$ then $a \equiv b \pmod{m}$.

Proof. If $ka - kb \vdots m$, then $k(a - b) \vdots m$. If $\gcd(k, m) = 1$ then $(a - b) \vdots m$.

Properties (what about the division?)

4) If $ka \equiv kb \pmod{m}$ and $\gcd(k, m) = 1$ then $a \equiv b \pmod{m}$.

Proof. If $ka - kb \vdots m$, then $k(a - b) \vdots m$. If $\gcd(k, m) = 1$ then $(a - b) \vdots m$.

Note that if $ka \equiv kb \pmod{m}$ then the congruence $a \equiv b \pmod{m}$ may not hold.
For example, $24 \equiv 16 \pmod{8}$ but it is not true that $3 \equiv 2 \pmod{8}$.

…So what?

In fact, we want to prove a statement like:

The residue of a sum equals to the sum of the residues.

Indeed, this is often true:

45 gives residue 3 modulo 7, 57 gives residue 1 modulo 7,

and 45+57=102 gives residue 3+1=4 modulo 7.

But:

61 gives residue 5 modulo 7, 25 gives residue 4 modulo 7,

And 61+25=86 gives residue 2, not 5+4=9 modulo 7.

...So what?

In fact, we want to prove a statement like:

The residue of a sum equals to the sum of the residues.

But:

61 gives residue 5 modulo 7, 25 gives residue 4 modulo 7,

And 61+25=86 gives residue 2, not 5+4=9 modulo 7.

So we write instead:

$$61 + 25 \equiv 5 + 4 \equiv 9 \equiv 2 \pmod{7}.$$

Example

Find the residue of $3333^{4444} + 4444^{3333}$ modulo 7.

Firstly, let's find the residues of the numbers 3333^{4444} and 4444^{3333}.

According to property 3, $3333 \equiv 1 \pmod 7$ and thus $3333^{4444} \equiv 1^{4444} \equiv 1 \pmod 7$.

In the same way, $4444 \equiv 6 \pmod 7$ and thus $4444^{3333} \equiv 6^{3333} \pmod 7$.

But what is the residue of $6^{3333} \pmod 7$?

Example

But what is the residue of 6^{3333} (mod 7)?

$6^1 = 6 \equiv 6 \pmod{7}$.

$6^2 = 36 \equiv 1 \pmod{7}$.

$6^3 = 216 \equiv 6 \pmod{7}$.

$6^4 = 1296 \equiv 1 \pmod{7}$.

Do you see the pattern?

Thus, $6^{3333} \equiv 6 \pmod{7}$.

Finally, the residue of $3333^{4444} + 4444^{3333}$ modulo 7 equals to 0.

Divisibility by 3

As you, probably, know, a number is divisible by 3 if and only if the sum of its digits is divisible by 3. But how does it work?

$$5812 = 5 \times 10^3 + 8 \times 10^2 + 1 \times 10 + 2 =$$

$$65347 = 6 \times 10^4 + 5 \times 10^3 + 3 \times 10^2 + 4 \times 10 + 7 =$$

Divisibility by 3

As you, probably, know, a number is divisible by 3 if and only if the sum of its digits is divisible by 3. But how does it work?

$$5812 = 5 \times 10^3 + 8 \times 10^2 + 1 \times 10 + 2 =$$

$$= 5 \times (999 + 1) + 8 \times (99 + 1) + 1 \times (9 + 1) + 2 =$$

$$65347 = 6 \times 10^4 + 5 \times 10^3 + 3 \times 10^2 + 4 \times 10 + 7 =$$

$$= 6 \times (999 + 1) + 5 \times (999 + 1) + 3 \times (99 + 1) + 4 \times (9 + 1) + 7 =$$

Divisibility by 3

As you, probably, know, a number is divisible by 3 if and only if the sum of its digits is divisible by 3. But how does it work?

$$5812 = 5 \times 10^3 + 8 \times 10^2 + 1 \times 10 + 2 =$$

$$= 5 \times (999 + 1) + 8 \times (99 + 1) + 1 \times (9 + 1) + 2 =$$

$$65347 = 6 \times 10^4 + 5 \times 10^3 + 3 \times 10^2 + 4 \times 10 + 7 =$$

$$= 6 \times (999 + 1) + 5 \times (999 + 1) + 3 \times (99 + 1) + 4 \times (9 + 1) + 7 =$$

Divisibility by 3

As you, probably, know, a number is divisible by 3 if and only if the sum of its digits is divisible by 3. But how does it work?

$$5812 = 5 \times 10^3 + 8 \times 10^2 + 1 \times 10 + 2 =$$

$$= 5 \times (999 + 1) + 8 \times (99 + 1) + 1 \times (9 + 1) + 2 =$$

$$= 5 \times 1 + 8 \times 1 + 1 \times 1 + 2 = 5 + 8 + 1 + 2 = 16,$$

$$65347 = 6 \times 10^4 + 5 \times 10^3 + 3 \times 10^2 + 4 \times 10 + 7 =$$

$$= 6 \times (999 + 1) + 5 \times (999 + 1) + 3 \times (99 + 1) + 4 \times (9 + 1) + 7 =$$

$$= 6 \times 1 + 5 \times 1 + 3 \times 1 + 4 \times 1 + 7 = 6 + 5 + 3 + 4 + 7 = 25.$$

Divisibility by 3

As you, probably, know, a number is divisible by 3 if and only if the sum of its digits is divisible by 3. But how does it work?

$$5812 = 5 \times 10^3 + 8 \times 10^2 + 1 \times 10 + 2 =$$

$$= 5 \times (999 + 1) + 8 \times (99 + 1) + 1 \times (9 + 1) + 2 =$$

$$= 5 \times 1 + 8 \times 1 + 1 \times 1 + 2 = 5 + 8 + 1 + 2 = 16,$$

$$65347 = 6 \times 10^4 + 5 \times 10^3 + 3 \times 10^2 + 4 \times 10 + 7 =$$

$$= 6 \times (999 + 1) + 5 \times (999 + 1) + 3 \times (99 + 1) + 4 \times (9 + 1) + 7 =$$

$$= 6 \times 1 + 5 \times 1 + 3 \times 1 + 4 \times 1 + 7 = 6 + 5 + 3 + 4 + 7 = 25.$$

One More Consequence

Let’s prove that a perfect square never gives residue 2 modulo 3.

One More Consequence

Let’s prove that a perfect square never gives residue 2 modulo 3.

Indeed, the residues modulo 3 of the numbers

1, 4, 9, 16, 25, 36, 49, 64, 81

are equal respectively to

1, 1, 0, 1, 1, 0, 1, 1, 0.

One More Consequence

Let’s prove that a perfect square never gives residue 2 modulo 3.

Indeed, the residues modulo 3 of the numbers

1, 4, 9, 16, 25, 36, 49, 64, 81

are equal respectively to

1, 1, 0, 1, 1, 0, 1, 1, 0.

Why does it happen? In fact, a perfect square is a number of the form $a \times a$, and we know that, if we are interested in the remainder modulo 3, then we can replace the both multipliers with their remainders modulo 3.

One More Consequence

Let’s prove that a perfect square never gives residue 2 modulo 3.

Indeed, the residues modulo 3 of the numbers

$$1,\ 4,\ 9,\ 16,\ 25,\ 36,\ 49,\ 64,\ 81$$

are equal respectively to

$$1,\ 1,\ 0,\ 1,\ 1,\ 0,\ 1,\ 1,\ 0.$$

Why does it happen? In fact, a perfect square is a number of the form $a \times a$, and we know that, if we are interested in the remainder modulo 3, then we can replace the both multipliers with their remainders modulo 3.

In such a way we get $0 \times 0 = 0$, or $1 \times 1 = 1$, or $2 \times 2 = 4 = 1$.

One More Consequence

A perfect square never gives residue 2 modulo 3.

And what happens to the remainders modulo 5?

If we are interested in the remainder modulo 5, then we can replace the both multipliers with their remainders modulo 5.

One More Consequence

A perfect square never gives residue 2 modulo 3.

And what happens to the remainders modulo 5?

If we are interested in the remainder modulo 5, then we can replace the both multipliers with their remainders modulo 5.

There are the possible cases:

$$0 \times 0 = 0 \qquad 1 \times 1 = 1 \qquad 2 \times 2 = 4$$

$$3 \times 3 = 9 = 4 \qquad 4 \times 4 = 16 = 1$$

One More Consequence

A perfect square never gives residue 2 modulo 3.

And what happens to the remainders modulo 5?

If we are interested in the remainder modulo 5, then we can replace the both multipliers with their remainders modulo 5.

There are the possible cases:

$$0 \times 0 = 0 \qquad 1 \times 1 = 1 \qquad 2 \times 2 = 4$$

$$3 \times 3 = 9 = 4 \qquad 4 \times 4 = 16 = 1$$

Thus, a perfect square can give remainders 0, 1 and 4 modulo 5, but cannot give remainder 2 or 3.

One More Difficult Example

Find the residue of 2^{102} modulo 101.

$2^1 = 2 \equiv 2 \pmod{101}$.

$2^2 = 4 \equiv 4 \pmod{101}$.

$2^3 = 8 \equiv 8 \pmod{101}$.

$2^4 = 16 \equiv 16 \pmod{101}$.

$2^5 = 32 \equiv 32 \pmod{101}$.

$2^6 = 64 \equiv 64 \pmod{101}$.

$2^7 = 128 \equiv 27 \pmod{101}$.

$2^8 = 256 \equiv 54 \pmod{101}$.

$2^9 = 512 \equiv 7 \pmod{101}$.

$2^{10} = 1024 \equiv 14 \pmod{101}$.

$2^{11} = 2048 \equiv 28 \pmod{101}$.

$2^{12} = 4096 \equiv 56 \pmod{101}$.

$2^{13} = 8192 \equiv 11 \pmod{101}$.

$2^{14} = 16384 \equiv 22 \pmod{101}$…???

Fermat’s Little Theorem

Let a be an integer and p be a prime such that gcd(a, p) = 1. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fermat’s Little Theorem

Let a be an integer and p be a prime such that gcd(a, p) = 1. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Try to use!

$2^{100} \equiv 1 \pmod{101}$. Thus, $2^{102} = 2^{100} \times 2^2 = 2^{100} \times 4 \equiv 1 \times 4 \pmod{101}$.

Thus, the residue of 2^{102} modulo 101 equals to 4.

Fermat’s Little Theorem

Let a be an integer and p be a prime such that gcd(a, p) = 1. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Important Lemma. Let gcd(m, n) = 1. Then the numbers m, $2m$, $3m$, …, nm give different residues modulo n.

Fermat’s Little Theorem

Let a be an integer and p be a prime such that gcd(a, p) = 1. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Important Lemma. Let gcd(m, n) = 1. Then the numbers m, $2m$, $3m$, …, nm give different residues modulo n.

For example, let $m = 9$, $n = 7$. Then we take the following numbers:

$$9, \quad 18, \quad 27, \quad 36, \quad 45, \quad 54, \quad 63$$

Fermat’s Little Theorem

Let a be an integer and p be a prime such that gcd(a, p) = 1. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Important Lemma. Let gcd(m, n) = 1. Then the numbers m, $2m$, $3m$, …, nm give different residues modulo n.

For example, let m = 9, n = 7. Then we take the following numbers:

$$9, \quad 18, \quad 27, \quad 36, \quad 45, \quad 54, \quad 63$$

The residues modulo 7 are:

$$2, \quad 4, \quad 6, \quad 1, \quad 3, \quad 5, \quad 0.$$

Fermat’s Little Theorem

Let a be an integer and p be a prime such that $\gcd(a, p) = 1$. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Important Lemma. Let $\gcd(m, n) = 1$. Then the numbers $m, 2m, 3m, \dots, nm$ give different residues modulo n.

Suppose there are two numbers, km and lm, where $1 \le k < l \le n$, which give the same residues modulo n. Then

$$lm - km \vdots n, \quad m(l - k) \vdots n, l - k \vdots n,$$

which is impossible since $1 \le k < l \le n$ and thus $0 < l - k < n$.

Fermat's Little Theorem

Let a be an integer and p be a prime such that $\gcd(a, p) = 1$. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Important Lemma. Let $\gcd(m, n) = 1$. Then the numbers $m, 2m, 3m, \ldots, nm$ give different residues modulo n.

Consider the numbers $a, 2a, 3a, \ldots, (p-1)a$.

$$a \times 2a \times 3a \times \ldots \times (p-1)a = (p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}.$$

$$a^{p-1} \equiv 1 \pmod{p}.$$

Another More Difficult Example

Find the residue of 2^{102} modulo 303.

There is a problem. The number 303 is not a prime: 303 = 101 × 3. Thus, the Fermat’s Little Theorem cannot be used.

Another More Difficult Example

Find the residue of 2^{102} modulo 303.

There is a problem. The number 303 is not a prime: $303 = 101 \times 3$. Thus, the Fermat's Little Theorem cannot be used.

But we know that $2^{102} \equiv 4 \pmod{101}$. Moreover, we can easily find the residue of 2^{102} modulo 3:

$2^1 = 2 \equiv 2 \pmod{3}$.

$2^2 = 4 \equiv 1 \pmod{3}$.

$2^3 = 8 \equiv 2 \pmod{3}$.

$2^4 = 16 \equiv 1 \pmod{3}$.

…

$2^{102} \equiv 1 \pmod{3}$.

Another More Difficult Example

Find the residue of 2^{102} modulo 303.

There is a problem. The number 303 is not a prime: $303 = 101 \times 3$. Thus, the Fermat's Little Theorem cannot be used.

But we know that $2^{102} \equiv 4 \pmod{101}$ and $2^{102} \equiv 1 \pmod{3}$.

If a number gives residue 4 modulo 101, then it gives one of the remainders 4, 105 or 206 modulo 303. Moreover, if this number gives the residue 1 modulo 3, then the remainder is 4.

Chinese Remainder Theorem

Suppose $m_1, m_2, \ldots, m_k$ are naturals such that gcd(m_i, m_j) =1 if $i \neq j$, and $r_1, r_2, \ldots, r_k$ are integers such that $0 \leq r_i < m_i$, $i = 1, 2, 3, \ldots, k$. Then there exists a natural N such that

$$N \equiv r_1 \pmod{m_1}, \quad N \equiv r_2 \pmod{m_2}, \quad \ldots, \quad N \equiv r_k \pmod{m_k}.$$

Chinese Remainder Theorem

Suppose m_1, m_2, …, m_k are naturals such that gcd(m_i, m_j) =1 if $i \neq j$, and r_1, r_2, …, r_k are integers such that $0 \leq r_i < m_i$, $i = 1, 2, 3, \ldots, k$. Then there exists a natural N such that

$$N \equiv r_1 \pmod{m_1},\ N \equiv r_2 \pmod{m_2},\qquad \ldots,\qquad N \equiv r_k \pmod{m_k}.$$

Why is it important that gcd(m_i, m_j) =1 if $i \neq j$?

Obviously, there is no such an integer N that

$$N \equiv 7 \pmod 8 \text{ and } N \equiv 12 \pmod{22}.$$

Chinese Remainder Theorem: Example – Proof.

Let’s find such an integer N that

$$N \equiv 2 \pmod{3}, \quad N \equiv 3 \pmod{5}, \quad N \equiv 3 \pmod{7}, \quad N \equiv 6 \pmod{11}.$$

Chinese Remainder Theorem: Example – Proof.

Let’s find such an integer N that

$$N \equiv 2 \pmod{3}, \quad N \equiv 3 \pmod{5}, \quad N \equiv 3 \pmod{7}, \quad N \equiv 6 \pmod{11}.$$

To begin with, let’s take a number N such that $N \equiv 2 \pmod{3}$, say, 2.

Chinese Remainder Theorem: Example – Proof.

Let's find such an integer N that

$$N \equiv 2 \pmod{3}, \quad N \equiv 3 \pmod{5}, \quad N \equiv 3 \pmod{7}, \quad N \equiv 6 \pmod{11}.$$

To begin with, let's take a number N such that $N \equiv 2 \pmod{3}$, say, 2.

Now we increase N by 3: 2, 5, 8.

Chinese Remainder Theorem: Example – Proof.

Let’s find such an integer N that

$$N \equiv 2 \pmod{3}, \quad N \equiv 3 \pmod{5}, \quad N \equiv 3 \pmod{7}, \quad N \equiv 6 \pmod{11}.$$

To begin with, let’s take a number N such that $N \equiv 2 \pmod{3}$, say, 2.

Now we increase N by 3: 2, 5, 8.

Now we increase N by 15: 8, 23, 38.

Chinese Remainder Theorem: Example – Proof.

Let’s find such an integer N that

$$N \equiv 2 \pmod{3}, \quad N \equiv 3 \pmod{5}, \quad N \equiv 3 \pmod{7}, \quad N \equiv 6 \pmod{11}.$$

To begin with, let’s take a number N such that $N \equiv 2 \pmod{3}$, say, 2.

Now we increase N by 3: 2, 5, 8.

Now we increase N by 15: 8, 23, 38.

Now we increase N by 105: 38, 143, 248.

One More Trick: Euclid’s Algorithm

Suppose a, b are two naturals and we have two find their greatest common divisor.

The algorithm is based on the following

Statement. If $a > b$ then $\gcd(a, b) = \gcd(a - b, b)$.

One More Trick: Euclid’s Algorithm

Statement. If $a > b$ then $\gcd(a, b) = \gcd(a - b, b)$.

Thus, we have the following algorithm:

$$\gcd(2057, 663) = \gcd(1394, 663) = \gcd(731, 663) = \gcd(68, 663) =$$

$$= \gcd(68, 595) = \gcd(68, 527) = \gcd(68, 459) = \gcd(68, 391) = \gcd(68, 323) =$$

$$= \gcd(68, 255) = \gcd(68, 187) = \gcd(68, 119) = \gcd(68, 51) = \gcd(17, 51) =$$

$$= \gcd(17, 34) = \gcd(17, 17) = 17.$$

One More Trick: Euclid’s Algorithm

Statement. If $a > b$ then $\gcd(a, b) = \gcd(a - b, b)$.

Thus, we have the following algorithm:

$$\gcd(2057, 663) = \gcd(1394, 663) = \gcd(731, 663) = \gcd(68, 663) =$$

$$= \gcd(68, 595) = \gcd(68, 527) = \gcd(68, 459) = \gcd(68, 391) = \gcd(68, 323) =$$

$$= \gcd(68, 255) = \gcd(68, 187) = \gcd(68, 119) = \gcd(68, 51) = \gcd(17, 51) =$$

$$= \gcd(17, 34) = \gcd(17, 17) = 17.$$

We can do it quicker. For example, here we subtract 68 from 663, while the obtained number is greater than 68. Obviously, we finally get the remainder of the number 663 modulo 68.

One More Trick: Euclid's Algorithm

Statement. If $a > b$ then $\gcd(a, b) = \gcd(a - b, b)$.

Thus, we have the following algorithm:

$$\gcd(2057, 663) = \gcd(68, 663) = \gcd(68, 51) = \gcd(17, 51) = 17.$$

We can do it quicker. For example, here we subtract 68 from 663, while the obtained number is greater than 68. Obviously, we finally get the remainder of the number 663 modulo 68.