Chapter 3 Basic Number Theory

What is Number Theory?

Well ...

What is Number Theory?

Well ...

Number Theory

The study of the natural numbers $(\mathcal{Z}^+)$, especially the relationship between different sorts of numbers.

What is Number Theory?

Well ...

Number Theory

The study of the natural numbers $(\mathcal{Z}^{+})$, especially the relationship between different sorts of numbers.

Divisibility

Suppose $n, m \in \mathcal{Z}, m \neq 0$, we say m divides n if n is a multiple of m. That is, $\exists\, k \in \mathcal{Z} \ni n = mk$. If m divides n, we write $m|n$. If not, $m \not| n$.

Basic Examples

- gcd(12,20)=

Greatest Common Factors

Basic Examples

- gcd(12,20)= 4
- gcd(18,30)=

Greatest Common Factors

Basic Examples

- gcd(12,20)= 4
- gcd(18,30)= 6
- gcd(225,120)=

Greatest Common Factors

Basic Examples

- gcd(12,20)= 4
- gcd(18,30)= 6
- gcd(225,120)= 15

Basic Examples

- gcd(12,20)= 4
- gcd(18,30)= 6
- gcd(225,120)= 15

For the last one, we cant just look at it and know the answer - we need some technique, and prime factorization works here.
$120 = 2^3 \cdot 3 \cdot 5$, $225 = 3^2 \cdot 5^2$

This is not practical for large numbers.

Example

Find $(132, 36)$

The Euclidean Algorithm

Example

Find $(132, 36)$

$$132 = 3 \cdot 36 + 24$$

The Euclidean Algorithm

Example

Find $(132, 36)$

$$\begin{aligned} 132 &= 3 \cdot 36 + 24 \\ 36 &= 1 \cdot 24 + 12 \end{aligned}$$

The Euclidean Algorithm

Example

Find $(132, 36)$

$$\begin{aligned} 132 &= 3 \cdot 36 + 24 \\ 36 &= 1 \cdot 24 + 12 \\ 24 &= 2 \cdot 12 + 0 \end{aligned}$$

The Euclidean Algorithm

Example

Find $(132, 36)$

$$\begin{aligned} 132 &= 3 \cdot 36 + 24 \\ 36 &= 1 \cdot 24 + 12 \\ 24 &= 2 \cdot 12 + 0 \end{aligned}$$

So, $(132, 36) = 12$.

Another Example

Example

Find $(1160718174, 316258250)$

Another Example

Example

Find $(1160718174, 316258250)$

The answer we seek is 1078.

Another Example

Example

Find $(1160718174, 316258250)$

The answer we seek is 1078.

Can you generalize this?

$(a, b) =$

Another Example

Example

Find $(1160718174, 316258250)$

The answer we seek is 1078.

Can you generalize this?

$(a, b) = (b, r)$

The Division Algorithm

Before we analyze, where does this equation come from? The division algorithm, which states

The Division Algorithm

Before we analyze, where does this equation come from? The division algorithm, which states

The Division Algorithm

$a = bq + r, 0 \leq r < b$

There are two parts to this proof, the existence of q and r, and uniqueness.

The Division Algorithm

Before we analyze, where does this equation come from? The division algorithm, which states

The Division Algorithm

$a = bq + r, 0 \leq r < b$

There are two parts to this proof, the existence of q and r, and uniqueness.

Proof

<u>Existence</u>

Consider the set $S = \{a - nd \mid n \in \mathcal{Z}\}$. We claim S contains a non-negative integer. There are two cases to consider:

1. If $a \geq 0$, choose $n = 0$
2. If $a < 0$, choose $n = ad$

The Division Algorithm Proof

Proof

In both cases, $a - nd$ is non-negative and thus S always contains at least one non-negative integer. This means we can apply the well-ordering principle.

The Division Algorithm Proof

Proof

In both cases, $a - nd$ is non-negative and thus S always contains at least one non-negative integer. This means we can apply the well-ordering principle.

> *Every non-empty set of positive integers contains a smallest element.*

The Division Algorithm Proof

Proof

In both cases, $a - nd$ is non-negative and thus S always contains at least one non-negative integer. This means we can apply the well-ordering principle.

> *Every non-empty set of positive integers contains a smallest element.*

and we can deduce that S contains a least non-negative integer r. By definition, $r = a - nd$ for some n. Let q be this n. Then, by rearranging, $a = qd + r$.

The Division Algorithm Proof

Proof

It remains to show $0 \leq r < |d|$. The first inequality holds as r was chosen to be non-negative. To show $r < |d|$, suppose $r \geq |d|$. Since $d \neq 0$, $r > 0$ but $d > 0$ or $d < 0$.

The Division Algorithm Proof

Proof

It remains to show $0 \leq r < |d|$. The first inequality holds as r was chosen to be non-negative. To show $r < |d|$, suppose $r \geq |d|$. Since $d \neq 0$, $r > 0$ but $d > 0$ or $d < 0$.

If $d > 0$ then $r \geq d$ implies $a - qd \geq d$, further implying $a - qd - d \geq 0 \Rightarrow a - (q+1)d \geq 0$. Therefore, $a - (q+1)d \in S$, and since $a - (q+1)d = r - d$ with $d > 0$, we know $a - (q+1)d < r$, contradicting that r was the least non-negative element in S.

The Division Algorithm Proof

Proof

It remains to show $0 \leq r < |d|$. The first inequality holds as r was chosen to be non-negative. To show $r < |d|$, suppose $r \geq |d|$. Since $d \neq 0$, $r > 0$ but $d > 0$ or $d < 0$.

If $d > 0$ then $r \geq d$ implies $a - qd \geq d$, further implying $a - qd - d \geq 0 \Rightarrow a - (q+1)d \geq 0$. Therefore, $a - (q+1)d \in S$, and since $a - (q+1)d = r - d$ with $d > 0$, we know $a - (q+1)d < r$, contradicting that r was the least non-negative element in S.

If $d < 0$, then $r \geq -d$ implies that $a - qd \geq -d$. This implies that $a - qd + d \geq 0 \Rightarrow a - (q-1)d \geq 0$. Therefore, $a - (q-1)d \in S$ and, since $a - (q-1)d = r + d$ with $d < 0$, we know $a - (q-1)d < r$. So, $r < |d|$, completing the existence proof.

The Division Algorithm Proof

Proof.

Uniqueness

Suppose there exists q, q', r, r' with $0 \leq r, r' < |d| \ni a = dq + r$ and $a = dq' + r'$. Without loss of generality, assume $q \leq q'$.

Subtracting the two equations yields $d(q' - q) = r - r'$.

The Division Algorithm Proof

Proof.

Uniqueness

Suppose there exists q, q', r, r' with $0 \leq r, r' < |d| \ni a = dq + r$ and $a = dq' + r'$. Without loss of generality, assume $q \leq q'$.
Subtracting the two equations yields $d(q' - q) = r - r'$.

If $d > 0$ then $r' \leq r$ and $r < d \leq d + r'$, so $(r - r') < d$. Similarly, if $d < 0$ then $r \leq r'$ and $r' < -d \leq -d + r$, so $-(r - r') < -d$.
Combining these yields $|r - r'| < |d|$.

The Division Algorithm Proof

Proof.

Uniqueness

Suppose there exists q, q', r, r' with $0 \leq r, r' < |d| \ni a = dq + r$ and $a = dq' + r'$. Without loss of generality, assume $q \leq q'$. Subtracting the two equations yields $d(q' - q) = r - r'$.

If $d > 0$ then $r' \leq r$ and $r < d \leq d + r'$, so $(r - r') < d$. Similarly, if $d < 0$ then $r \leq r'$ and $r' < -d \leq -d + r$, so $-(r - r') < -d$. Combining these yields $|r - r'| < |d|$.

The original equation implies $|d|$ divides $|r - r'|$. So, $|d| \leq |r - r'|$ or $|r - r'| = 0$. But, we established that $|r - r'| < |d|$, so $r = r'$. Substituting into the original equation yields $dq = dq'$ and since $d \neq 0$, $q = q'$, proving uniqueness.

$\square$

The Division Algorithm

Back to the Euclidean Algorithm. The general method looks like:

$$\begin{aligned}
a &= q_1 b + r_1 \\
b &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
r_2 &= q_4 r_3 + r_4 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + {\color{red} r_n} \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

Back to the Euclidean Algorithm. The general method looks like:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ r_2 &= q_4 r_3 + r_4 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + {\color{red} r_n} \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

Why is this last nonzero remainder r_n a common divisor of a and b?

The Division Algorithm

Back to the Euclidean Algorithm. The general method looks like:

$$\begin{aligned}
a &= q_1 b + r_1 \\
b &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
r_2 &= q_4 r_3 + r_4 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

Why is this last nonzero remainder r_n a common divisor of a and b?

Start from the bottom and work upwards.

Justification

The last line $r_{n-1} = q_{n+1} r_n$ shows that $r_n | r_{n-1}$.

Justification

The last line $r_{n-1} = q_{n+1}r_n$ shows that $r_n | r_{n-1}$.

The line above that $r_{n-2} = q_n r_{n-1} + r_n$ shows that r_n divides r_{n-2} since it divides r_n and r_{n-1}.

Justification

The last line $r_{n-1} = q_{n+1} r_n$ shows that $r_n | r_{n-1}$.

The line above that $r_{n-2} = q_n r_{n-1} + r_n$ shows that r_n divides r_{n-2} since it divides r_n and r_{n-1}.

By continuing in this fashion, we see it also divides $r_{n-3}, r_{n-4}, \cdots$, all the way through to a and b.

Justification

But, why is r_n the greatest common divisor of a and b?

Justification

But, why is r_n the greatest common divisor of a and b?

Suppose d is any common divisor of a and b. We will work our way back down the list. Consider $a = q_1 b + r_1$. Since d divides a and b, it must also divide r_1. The second equation $b = q_2 r_1 + r_2$ shows d must divide r_2.

Justification

But, why is r_n the greatest common divisor of a and b?

Suppose d is any common divisor of a and b. We will work our way back down the list. Consider $a = q_1 b + r_1$. Since d divides a and b, it must also divide r_1. The second equation $b = q_2 r_1 + r_2$ shows d must divide r_2.

Continuing down the line, at each stage we know d divides the previous two remainders, r_{i-1} and r_i, and the current line $r_{i-1} = q_{i+1} r_i + r_{i+1}$ will tell us d also divides r_{i+1}.

Justification

But, why is r_n the greatest common divisor of a and b?

Suppose d is any common divisor of a and b. We will work our way back down the list. Consider $a = q_1 b + r_1$. Since d divides a and b, it must also divide r_1. The second equation $b = q_2 r_1 + r_2$ shows d must divide r_2.

Continuing down the line, at each stage we know d divides the previous two remainders, r_{i-1} and r_i, and the current line $r_{i-1} = q_{i+1} r_i + r_{i+1}$ will tell us d also divides r_{i+1}.

Eventually, we reach $r_{n-2} = q_n r_{n-1} + r_n$, at which point we conclude $d | r_n$. So, if we have any common divisor of a and b in d then $d | r_n$. Therefore r_n must be the greatest common divisor of a and b.

The Division Algorithm

Statement of the Division Algorithm

To compute (a, b), let $r_{-1} = a$ and $r_0 = b$ and compute successive quotients and remainders of $r_{i-1} = q_{i+1} r_i + r_{i+1}$ until some remainder $r_{n+1} = 0$. Then r_n is the greatest common divisor.

Primes

Theorem

There are infinitely many primes.

Primes

Theorem

There are infinitely many primes.

Proof.

Suppose we start with a list of all primes $p_1, p_2, \cdots, p_n$. Let $A = p_1 p_2 \cdots p_n + 1$. A is larger than any number on our list. So, if A is prime then we are done.

Primes

Theorem

There are infinitely many primes.

Proof.

Suppose we start with a list of all primes $p_1, p_2, \cdots, p_n$. Let $A = p_1 p_2 \cdots p_n + 1$. A is larger than any number on our list. So, if A is prime then we are done.

If A is composite, then there must be a $q_1 \ni q_1 | A$ where $q_1 \neq p_i$ for all $i = 1, \cdots n$. Because $q_1 \not| 1$ we have a contradiction, So, it must be so that q_1 is a prime not on our original list.

Primes

Theorem

There are infinitely many primes.

Proof.

Suppose we start with a list of all primes $p_1, p_2, \cdots, p_n$. Let $A = p_1 p_2 \cdots p_n + 1$. A is larger than any number on our list. So, if A is prime then we are done.

If A is composite, then there must be a $q_1 \ni q_1 | A$ where $q_1 \neq p_i$ for all $i = 1, \cdots n$. Because $q_1 \not| 1$ we have a contradiction, So, it must be so that q_1 is a prime not on our original list.

Let $B = q_1 p_1 \cdots p_n + 1$ and repeat this process. $\square$

Theorem

If x_0, y_0 is a solution of $ax + by = c$, then so is $x_0 + bt, y_0 - at$.

Proof.

We know $ax_0 + by_0 = c$. Consider the following:

$$\begin{aligned} & a(x_0 + bt) + b(y_0 - at) \\ &= ax_0 + abt + by_0 - abt \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

$\square$

Helpful Tools for Number Theory

Theorem

If $(a, b) \nmid c$ then $ax + by = c$ has no solution and if $(a, b)|c$ then $ax + by = c$ has a solution.

Proof.

Suppose $\exists x_0, y_0 \in \mathcal{Z} \ni ax_0 + by_0 = c$. Since $(a, b)|ax_0$ and $(a, b)|by_0$, $(a, b)|c$.
Conversely, suppose $(a, b)|c$. then $c = m(a, b)$ for some m. We know $ar + bs = (a, b)$ for some $r, s \in \mathcal{Z}$. Then,

$$a(rm) + b(sm) = m(a, b) = c$$

and $x = rm, y = sm$ is a solution. $\square$

One More Theorem

Theorem

Suppose $(a, b) = 1$ *and* x_0, y_0 *is a solution of* $ax + by = c$*. Then all solutions are given by* $x = x_0 + bt, y = y_0 - at$ *for* $t \in \mathcal{Z}$.

Congruences

Definition

Let a, b, n be integers with $n \neq 0$, We say $a \equiv b \pmod{n}$ if $a - b$ is a multiple of n.

Congruences

Definition

Let a, b, n be integers with $n \neq 0$, We say $a \equiv b (\text{mod } n)$ if $a - b$ is a multiple of n.

The Linear Congruence Theorem

Suppose $g = (a, m)$.

a) If $g \not| b$ then $ax \equiv b (\text{mod } m)$ has no solutions.

b) If $g | b$ then $ax \equiv b (\text{mod } m)$ has exactly g incongruent solutions.

Proof of (a)

Proof.

(by contrapositive) If $ax \equiv b \pmod{m}$ has a solution then $(a, m) | b$. Suppose r is a solution. Then $ar \equiv b \pmod{m}$ by definition, and from the definition, $m | (ar - b)$, or $ar - b = km$ for some k. Since $(a, m) | a$ and $(a, m) | km$, it follows that $(a, m) | b$.

$\square$

Proof of (b)

Proof.

Since $g = (a, m)$ and $g|b$ then we can rewrite our congruence as

$$\frac{a}{g}x \equiv \frac{b}{g} \left(\mathrm{mod}\ \frac{m}{g}\right)$$

Proof of (b)

Proof.

Since $g = (a, m)$ and $g|b$ then we can rewrite our congruence as

$$\frac{a}{g}x \equiv \frac{b}{g} \left(\bmod \frac{m}{g}\right)$$

But, $\left(\frac{a}{g}, \frac{m}{g}\right)$=1, so the right hand side has a unique solution modulo $\frac{m}{g}$, say $x \equiv x_1 \left(\frac{m}{g}\right)$.

Proof of (b)

Proof.

Since $g = (a, m)$ and $g|b$ then we can rewrite our congruence as

$$\frac{a}{g}x \equiv \frac{b}{g} \left(\mod \frac{m}{g} \right)$$

But, $\left(\frac{a}{g}, \frac{m}{g}\right)$=1, so the right hand side has a unique solution modulo $\frac{m}{g}$, say $x \equiv x_1 \left(\frac{m}{g}\right)$.

So, the integers x which satisfy $ax \equiv b(\text{mod } m)$ are exactly those of the form $x = x_1 + k\frac{m}{g}$ for some k.

Proof of (b)

Proof.

Consider the set of integers

$$\left\{x_1, x_1 + \frac{m}{g}, x_1 + 2\frac{m}{g}, \cdots, x_1 + (g-1)\frac{m}{g}\right\}$$

Proof of (b)

Proof.

Consider the set of integers

$$\left\{x_1, x_1 + \frac{m}{g}, x_1 + 2\frac{m}{g}, \cdots, x_1 + (g-1)\frac{m}{g}\right\}$$

None of these are congruent modulo m and none differ by as much as m. further, for any $k \in \mathcal{Z}$, we have that $x_1 + k\frac{m}{g}$ is congruent modulo m to one of them.

Proof of (b)

Proof.

To see this, write $k = gq + r$ where $0 \leq r < d$ from the Division Algorithm. then,

$$\begin{aligned} & x_1 + k\frac{m}{g} \\ = {} & x_1 + (gq + r)\frac{m}{g} \\ = {} & x_1 + mq + r\frac{m}{g} \\ \equiv {} & x_1 + r\frac{m}{g} \pmod{m} \end{aligned}$$

So, these are the g solutions of $ax \equiv b \pmod{m}$. $\square$

Congruence Rules

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

Congruence Rules

1. $a \equiv a \pmod{m}$
2. $a \equiv 0 \pmod{m}$ iff $m|a$

Congruence Rules

1. $a \equiv a \pmod{m}$
2. $a \equiv 0 \pmod{m}$ iff $m|a$
3. $a \equiv b \pmod{m}$ iff $b \equiv a \pmod{m}$

Congruence Rules

1. $a \equiv a (\text{mod } m)$
2. $a \equiv 0 (\text{mod } m)$ iff $m | a$
3. $a \equiv b (\text{mod } m)$ iff $b \equiv a (\text{mod } m)$
4. If $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$ then
    1. $a + c \equiv b + d (\text{mod } m)$

Congruence Rules

1. $a \equiv a \pmod{m}$
2. $a \equiv 0 \pmod{m}$ iff $m|a$
3. $a \equiv b \pmod{m}$ iff $b \equiv a \pmod{m}$
4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
    1. $a + c \equiv b + d \pmod{m}$
    2. $ac \equiv bd \pmod{m}$

Congruence Rules

1. $a \equiv a \pmod{m}$
2. $a \equiv 0 \pmod{m}$ iff $m | a$
3. $a \equiv b \pmod{m}$ iff $b \equiv a \pmod{m}$
4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
    1. $a + c \equiv b + d \pmod{m}$
    2. $ac \equiv bd \pmod{m}$
5. $(a, n) = 1$ then $ab \equiv ac \pmod{n}$ implies that $b \equiv c \pmod{n}$

Congruence Rules

1. $a \equiv a \pmod{m}$
2. $a \equiv 0 \pmod{m}$ iff $m|a$
3. $a \equiv b \pmod{m}$ iff $b \equiv a \pmod{m}$
4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
    1. $a + c \equiv b + d \pmod{m}$
    2. $ac \equiv bd \pmod{m}$
5. $(a, n) = 1$ then $ab \equiv ac \pmod{n}$ implies that $b \equiv c \pmod{n}$
6. If $(a, n) = d \neq 1$ then $a \equiv b \pmod{n}$ implies $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$

Congruence Rules

1. $a \equiv a (\text{mod } m)$
2. $a \equiv 0 (\text{mod } m)$ iff $m|a$
3. $a \equiv b (\text{mod } m)$ iff $b \equiv a (\text{mod } m)$
4. If $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$ then
    1. $a + c \equiv b + d (\text{mod } m)$
    2. $ac \equiv bd (\text{mod } m)$
5. $(a, n) = 1$ then $ab \equiv ac (\text{mod } n)$ implies that $b \equiv c (\text{mod } n)$
6. If $(a, n) = d \neq 1$ then $a \equiv b (\text{mod } n)$ implies $\frac{a}{d} \equiv \frac{b}{d} (\text{mod } \frac{n}{d})$
7. If $(a, m) = 1$ then $ax \equiv b (\text{mod } m)$ has one solution.

Using These Properties

Example

Solve for x in $4x \equiv 3 \pmod{19}$.

Using These Properties

Example

Solve for x in $4x \equiv 3 \pmod{19}$.

Since $(5, 19) = 1$, we can multiply both sides by 5. This gives

$$4x \equiv 3 \pmod{19}$$
$$20x \equiv 15 \pmod{19}$$

and since $20 \equiv 1 \pmod{19}$, we have that $x \equiv 15 \pmod{19}$.

And Another One

Example

Solve for x in $6x \equiv 15 \pmod{514}$

And Another One

Example

Solve for x in $6x \equiv 15 \pmod{514}$

Since $6x - 15$ is always odd, it can never be divisible by 514. So, there is no solution.

Fermat's Little Theorem

Theorem

Let p be a prime which does not divide the integer a, then $a^{p-1} \equiv 1 (\bmod p)$.

Proof.

Start by listing the first $p - 1$ positive multiples of a:
$a, 2a, 3a, \cdots, (p-1)a.$

Fermat's Little Theorem

Theorem

Let p be a prime which does not divide the integer a, then $a^{p-1} \equiv 1 (\bmod p)$.

Proof.

Start by listing the first $p-1$ positive multiples of a:
$a, 2a, 3a, \cdots, (p-1)a$.
Suppose that ra and sa are the same modulo p, then we have $r \equiv s (\bmod p)$, so the $p-1$ multiples of a above are distinct and nonzero; that is, they must be congruent to $1, 2, 3, \cdots, p-1$ in some order.

Fermat's Little Theorem

Theorem

Let p be a prime which does not divide the integer a, then $a^{p-1} \equiv 1 (\text{mod } p)$.

Proof.

Start by listing the first $p-1$ positive multiples of a:
$a, 2a, 3a, \cdots, (p-1)a$.
Suppose that ra and sa are the same modulo p, then we have $r \equiv s (\text{mod } p)$, so the $p-1$ multiples of a above are distinct and nonzero; that is, they must be congruent to $1, 2, 3, \cdots, p-1$ in some order.
Multiply all these congruences together and we find

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot (p-1) (\text{mod } p)$$

or better, $a^{p-1}(p-1)! \equiv (p-1)! (\text{mod } p)$. Divide both sides by $(p-1)!$ to complete the proof. □