

CS103A

10/27/08

If you want a text:

Kenneth Rosen
Discrete Mathematics and Its Applications, 6th Ed.

Some properties of gcd

If $a = bq + r$ for integers $a, b, q,$ and $r,$
then $\gcd(a, b) = \gcd(b, r).$

$\gcd(66, 45) = \gcd(45, 21)$

Theorem 32.4 (proved in the handout)

Some properties of gcd

The GCD Identity (Bézout's Identity)
If $\gcd(a, b) = d,$ then there exist integers
 m and n such that $d = am + bn.$

Some properties of gcd

The GCD Identity (Bézout's Identity)
If $\gcd(a, b) = d,$ then there exist integers
 m and n such that $d = am + bn.$

$a = 66, b = 45$

	m	n	d
-3	-3	-333	
-2	-3	-267	
-1	-3	-201	
0	-3	-135	
1	-3	-69	
2	-3	-3	
3	-3	63	
-3	-2	-288	
-2	-2	-222	
-1	-2	-156	
0	-2	-90	
1	-2	-24	
2	-2	42	
3	-2	108	

Some properties of gcd

The GCD Identity (Bézout's Identity)
If $\gcd(a, b) = d,$ then there exist integers
 m and n such that $d = am + bn.$

$a = 66, b = 45$

	n						
	-3	-2	-1	0	1	2	3
-3	-333	-288	-243	-198	-153	-108	-63
-2	-267	-222	-177	-132	-87	-42	3
-1	-201	-156	-111	-66	-21	24	69
m 0	-135	-90	-45	0	45	90	135
1	-69	-24	21	66	111	156	201
2	-3	42	87	132	177	222	267
3	63	108	153	198	243	288	333

$-1 \cdot 66 + 2 \cdot 45$

Some properties of gcd

The GCD Identity (Bézout's Identity)
If $\gcd(a, b) = d,$ then there exist integers
 m and n such that $d = am + bn.$

$a = 66, b = 45$

	n						
	-3	-2	-1	0	1	2	3
-3	-333	-288	-243	-198	-153	-108	-63
-2	-267	-222	-177	-132	-87	-42	3
-1	-201	-156	-111	-66	-21	24	69
m 0	-135	-90	-45	0	45	90	135
1	-69	-24	21	66	111	156	201
2	-3	42	87	132	177	222	267
3	63	108	153	198	243	288	333

$-2 \cdot 66 + 3 \cdot 45$

Some properties of gcd

The GCD Identity (Bézout's Identity)
 If $\gcd(a, b) = d$, then there exist integers m and n such that $d = am + bn$.

$a = 66, b = 45$

		n						
		-3	-2	-1	0	1	2	3
m	-3	-333	-288	-243	-198	-153	-108	-63
	-2	-267	-222	-177	-132	-87	-42	3
	-1	-201	-156	-111	-66	-21	24	69
	0	-135	-90	-45	0	45	90	135
	1	-69	-24	21	66	111	156	201
	2	-3	42	87	132	177	222	267
	3	63	108	153	198	243	288	333

$\gcd(66, 45) = -2 \cdot 66 + 3 \cdot 45 = 3$

If $\gcd(a, b) = d$, then there exist integers m and n such that $d = am + bn$. (a and b are not both 0.)

PROOF: Let S be the set of all positive integers of the form $am + bn$, and let $k = au + bv$ be the smallest member of S . (We need to argue that S is not empty and that it has a smallest member).

If $\gcd(a, b) = d$, then there exist integers m and n such that $d = am + bn$. (a and b are not both 0.)

PROOF: Let S be the set of all positive integers of the form $am + bn$, and let $k = au + bv$ be the smallest member of S . (We need to argue that S is not empty and that it has a smallest member).

First we show that $k \mid a$ and $k \mid b$.

If $\gcd(a, b) = d$, then there exist integers m and n such that $d = am + bn$. (a and b are not both 0.)

PROOF: Let S be the set of all positive integers of the form $am + bn$, and let $k = au + bv$ be the smallest member of S . (We need to argue that S is not empty and that it has a smallest member).

First we show that $k \mid a$ and $k \mid b$. If $a = 0$, then $k \mid a$.

If $\gcd(a, b) = d$, then there exist integers m and n such that $d = am + bn$. (a and b are not both 0.)

PROOF: Let S be the set of all positive integers of the form $am + bn$, and let $k = au + bv$ be the smallest member of S . (We need to argue that S is not empty and that it has a smallest member).

First we show that $k \mid a$ and $k \mid b$. If $a = 0$, then $k \mid a$. If $a \neq 0$, then there are integers q and r such that $a = kq + r$ with $0 \leq r < k$, by the Division Theorem. So $r = a - kq$

$$= a - (au + bv)q$$

$$= a(1 - uq) + b(-vq)$$

If $\gcd(a, b) = d$, then there exist integers m and n such that $d = am + bn$. (a and b are not both 0.)

PROOF: Let S be the set of all positive integers of the form $am + bn$, and let $k = au + bv$ be the smallest member of S . (We need to argue that S is not empty and that it has a smallest member).

First we show that $k \mid a$ and $k \mid b$. If $a = 0$, then $k \mid a$. If $a \neq 0$, then there are integers q and r such that $a = kq + r$ with $0 \leq r < k$, by the Division Theorem. So $r = a - kq$

$$= a - (au + bv)q$$

$$= a(1 - uq) + b(-vq)$$

So r is a linear combination of a and b .

If $\gcd(a, b) = d$, then there exist integers m and n such that $d = am + bn$. (a and b are not both 0.)

PROOF: Let S be the set of all positive integers of the form $am + bn$, and let $k = au + bv$ be the smallest member of S . (We need to argue that S is not empty and that it has a smallest member).

First we show that $k \mid a$ and $k \mid b$. If $a = 0$, then $k \mid a$. If $a \neq 0$, then there are integers q and r such that $a = kq + r$ with $0 \leq r < k$, by the Division Theorem. So $r = a - kq$

$$= a - (au + bv)q$$

$$= a(1 - uq) + b(-vq)$$

So r is a linear combination of a and b . Since k is the smallest positive linear combination, and $0 \leq r < k$, it must be the case that $r = 0$.

Thus $a = kq$, and $k \mid a$. By a similar argument, $k \mid b$.

If $\gcd(a, b) = d$, then there exist integers m and n such that $d = am + bn$. (a and b are not both 0.)

PROOF: Let S be the set of all positive integers of the form $am + bn$, and let $k = au + bv$ be the smallest member of S . (We need to argue that S is not empty and that it has a smallest member).

First we show that $k \mid a$ and $k \mid b$. If $a = 0$, then $k \mid a$. If $a \neq 0$, then there are integers q and r such that $a = kq + r$ with $0 \leq r < k$, by the Division Theorem. So $r = a - kq$

$$= a - (au + bv)q$$

$$= a(1 - uq) + b(-vq)$$

So r is a linear combination of a and b . Since k is the smallest positive linear combination, and $0 \leq r < k$, it must be the case that $r = 0$.

Thus $a = kq$, and $k \mid a$. By a similar argument, $k \mid b$.

Now we show that $k = d$. Since $d \mid a$ and $d \mid b$, there are integers f and g such that $a = df$ and $b = dg$.

If $\gcd(a, b) = d$, then there exist integers m and n such that $d = am + bn$. (a and b are not both 0.)

PROOF: Let S be the set of all positive integers of the form $am + bn$, and let $k = au + bv$ be the smallest member of S . (We need to argue that S is not empty and that it has a smallest member).

First we show that $k \mid a$ and $k \mid b$. If $a = 0$, then $k \mid a$. If $a \neq 0$, then there are integers q and r such that $a = kq + r$ with $0 \leq r < k$, by the Division Theorem. So $r = a - kq$

$$= a - (au + bv)q$$

$$= a(1 - uq) + b(-vq)$$

So r is a linear combination of a and b . Since k is the smallest positive linear combination, and $0 \leq r < k$, it must be the case that $r = 0$.

Thus $a = kq$, and $k \mid a$. By a similar argument, $k \mid b$.

Now we show that $k = d$. Since $d \mid a$ and $d \mid b$, there are integers f and g such that $a = df$ and $b = dg$. So $k = dfu + dg v = d(fu + gv)$.

If $\gcd(a, b) = d$, then there exist integers m and n such that $d = am + bn$. (a and b are not both 0.)

PROOF: Let S be the set of all positive integers of the form $am + bn$, and let $k = au + bv$ be the smallest member of S . (We need to argue that S is not empty and that it has a smallest member).

First we show that $k \mid a$ and $k \mid b$. If $a = 0$, then $k \mid a$. If $a \neq 0$, then there are integers q and r such that $a = kq + r$ with $0 \leq r < k$, by the Division Theorem. So $r = a - kq$

$$= a - (au + bv)q$$

$$= a(1 - uq) + b(-vq)$$

So r is a linear combination of a and b . Since k is the smallest positive linear combination, and $0 \leq r < k$, it must be the case that $r = 0$.

Thus $a = kq$, and $k \mid a$. By a similar argument, $k \mid b$.

Now we show that $k = d$. Since $d \mid a$ and $d \mid b$, there are integers f and g such that $a = df$ and $b = dg$. So $k = dfu + dg v = d(fu + gv)$. k and d are positive, so $fu + gv$ is positive and $d \leq k$.

If $\gcd(a, b) = d$, then there exist integers m and n such that $d = am + bn$. (a and b are not both 0.)

PROOF: Let S be the set of all positive integers of the form $am + bn$, and let $k = au + bv$ be the smallest member of S . (We need to argue that S is not empty and that it has a smallest member).

First we show that $k \mid a$ and $k \mid b$. If $a = 0$, then $k \mid a$. If $a \neq 0$, then there are integers q and r such that $a = kq + r$ with $0 \leq r < k$, by the Division Theorem. So $r = a - kq$

$$= a - (au + bv)q$$

$$= a(1 - uq) + b(-vq)$$

So r is a linear combination of a and b . Since k is the smallest positive linear combination, and $0 \leq r < k$, it must be the case that $r = 0$.

Thus $a = kq$, and $k \mid a$. By a similar argument, $k \mid b$.

Now we show that $k = d$. Since $d \mid a$ and $d \mid b$, there are integers f and g such that $a = df$ and $b = dg$. So $k = dfu + dg v = d(fu + gv)$. k and d are positive, so $fu + gv$ is positive and $d \leq k$. But d is the greatest common divisor of a and b , so we must have $k = d$. Thus choosing k as above provides us with a linear combination of a and b equal to $\gcd(a, b)$. QED.

If $\gcd(a, b) = d$, then there exist integers m and n such that $d = am + bn$. (a and b are not both 0.)

$$3 = 66(-2) + 45(3)$$

PROOF: Let S be the set of all positive integers of the form $am + bn$, and let $k = au + bv$ be the smallest member of S . (We need to argue that S is not empty and that it has a smallest member).

$$3 \mid 66 \text{ and } 3 \mid 45$$

First we show that $k \mid a$ and $k \mid b$. If $a = 0$, then $k \mid a$. If $a \neq 0$, then there are integers q and r such that $a = kq + r$ with $0 \leq r < k$, by the Division Theorem. So $r = a - kq$

$$= a - (au + bv)q$$

$$= a(1 - uq) + b(-vq)$$

So r is a linear combination of a and b . Since k is the smallest positive linear combination, and $0 \leq r < k$, it must be the case that $r = 0$.

Thus $a = kq$, and $k \mid a$. By a similar argument, $k \mid b$.

$$66 = 3(22) \quad 45 = 3(15) \quad 3 = 3(22(-2) + 15(3))$$

Now we show that $k = d$. Since $d \mid a$ and $d \mid b$, there are integers f and g such that $a = df$ and $b = dg$. So $k = dfu + dg v = d(fu + gv)$. k and d are positive, so $fu + gv$ is positive and $d \leq k$. But d is the greatest common divisor of a and b , so we must have $k = d$. Thus choosing k as above provides us with a linear combination of a and b equal to $\gcd(a, b)$. QED.

Prime Numbers

The statement that an integer $n > 1$ is **prime** means that if $n = rs$ for positive integers r and s , then $r = 1$ or $s = 1$.

That is, the only divisors of n are itself and 1.

The statement that an integer $n > 1$ is **composite** means that n is not prime.

That is, $n = rs$ for some positive integers r and s with $r \neq 1$ and $s \neq 1$.

Some Theorems Involving Prime Numbers

Theorem: If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Some Theorems Involving Prime Numbers

Theorem: If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

PROOF: Suppose $p \nmid a$. Then since p is prime, the only common divisor of p and a is 1; i.e., $\gcd(p, a) = 1$. By the GCD Identity there exist integers x and y such that

$$1 = px + ay$$

$$b = pbx + aby$$

So $b = pbx + aby$

But $p \mid pbx$ and $p \mid aby$, so $p \mid b$.

Thus $p \mid a$ or $p \mid b$. QED.

Another form of this theorem: If $c \mid ab$ and $\gcd(c, a) = 1$, then $c \mid b$.

Some Theorems Involving Prime Numbers

Theorem: If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Theorem: If p is prime and $p \mid a_1 a_2 \dots a_n$, then $p \mid a_i$ for some i .

Some Theorems Involving Prime Numbers

Theorem: If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Theorem: If p is prime and $p \mid a_1 a_2 \dots a_n$, then $p \mid a_i$ for some i .

The Fundamental Theorem of Arithmetic:

Every positive integer greater than 1 can be written uniquely as the product of primes. (Note: a prime number p is considered to be, by itself, a product with a single term, and we mean unique except for the ordering of the primes in the product.)

$$8100 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 = 2^2 \cdot 3^4 \cdot 5^2$$

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

Some Theorems Involving Prime Numbers

Theorem: An integer $n > 1$ is composite if and only if it has a prime divisor $\leq \sqrt{n}$.

Proof: Suppose n is divisible by prime $p \leq \sqrt{n}$. Then there must be an integer r such that $pr = n$. Thus n is composite.

Suppose n is composite. Then $n = ab$, where $1 < a < n$ and $1 < b < n$. At least one of a and b is $\leq \sqrt{n}$ (if not, $ab > n$), and this factor is divisible by a prime p , which then divides n .

$\text{floor}(x)$ = the unique integer n such that $n \leq x < n + 1$
 $\text{ceil}(x)$ = the unique integer $n + 1$ such that $n < x \leq n + 1$

Testing for Primality

```

Prime(n)    n is an integer > 1
{
  for (a := 2, a ≤ floor(sqrt(n)), a := a + 1)
  {
    if ((n mod a) = 0)
    {
      return FALSE
    }
  }
  return TRUE
}
    
```

Testing for Primality

For numbers like $2^{24,036,583} - 1$ we need better algorithms.

Search on "largest prime"
 "Miller-Rabin test"
 "GIMPS"

Testing for Primality

Some simple tests:

- n is divisible by 2 if the rightmost digit is divisible by 2
- by 3 if the sum of the digits is divisible by 3
- by 4 if the number consisting of the last 2 digits is divisible by 4
- by 5 if the rightmost digit is 0 or 5
- by 9 if the sum of the digits is divisible by 9
- by 11 if the alternating sum of the digits is divisible by 11

$n = 2149719 \quad 9 - 1 + 7 - 9 + 4 - 1 + 2 = 11$

$$\frac{2149719}{11} = 195429$$

The Modulus Operator and Congruence

If a and m are integers with $m > 0$, then the remainder of a divided by m is denoted by $a \bmod m$.

The Modulus Operator and Congruence

If a and m are integers with $m > 0$, then the remainder of a divided by m is denoted by $a \bmod m$.

When we write $a = qm + r$, $0 \leq r < m$, then $r = a \bmod m$.

This makes it clear that for a given integer m , the possible values of $a \bmod m$ are

$0, 1, 2, \dots, m - 1$

The Modulus Operator and Congruence

If a and m are integers with $m > 0$, then the remainder of a divided by m is denoted by $a \bmod m$.

When we write $a = qm + r$, $0 \leq r < m$, then $r = a \bmod m$.

This makes it clear that for a given integer m , the possible values of $a \bmod m$ are

$0, 1, 2, \dots, m - 1$

$m = 7$

a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
$a \bmod 7$	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	...

The Modulus Operator and Congruence

If a and m are integers with $m > 0$, then the remainder of a divided by m is denoted by $a \bmod m$.

When we write $a = qm + r$, $0 \leq r < m$, then $r = a \bmod m$.

This makes it clear that for a given integer m , the possible values of $a \bmod m$ are

$0, 1, 2, \dots, m - 1$

$m = 7$

a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
$a \bmod 7$	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	...

The Modulus Operator and Congruence

If a and m are integers with $m > 0$, then the remainder of a divided by m is denoted by $a \bmod m$.

When we write $a = qm + r$, $0 \leq r < m$, then $r = a \bmod m$.

This makes it clear that for a given integer m , the possible values of $a \bmod m$ are

$0, 1, 2, \dots, m - 1$

$m = 7$

a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
$a \bmod 7$	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	...

The Modulus Operator and Congruence

The statement that a is congruent to b modulo m means that m divides $a - b$. We use the notation $a \equiv b \pmod{m}$, and we say that a and b are in the same congruence class.

The Modulus Operator and Congruence

The statement that a is congruent to b modulo m means that m divides $a - b$. We use the notation $a \equiv b \pmod{m}$, and we say that a and b are in the same congruence class.

Theorem: If a and b are integers and m is a positive integer, then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$. That is, a and b are congruent modulo m if and only if they have the same remainders when they are divided by m .

The Modulus Operator and Congruence

The statement that a is congruent to b modulo m means that m divides $a - b$. We use the notation $a \equiv b \pmod{m}$, and we say that a and b are in the same congruence class.

Theorem: If a and b are integers and m is a positive integer, then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$. That is, a and b are congruent modulo m if and only if they have the same remainders when they are divided by m .

$a \bmod 7$	0	1	2	3	4	5	6
a	0	1	2	3	4	5	6
	7	8	9	10	11	12	13
	14	15	16	17	18	19	20
	21	22	23	24	25	26	27
	28	29	30	31	32	33	34

The Modulus Operator and Congruence

The statement that a is congruent to b modulo m means that m divides $a - b$. We use the notation $a \equiv b \pmod{m}$, and we say that a and b are in the same congruence class.

Theorem: If a and b are integers and m is a positive integer, then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$. That is, a and b are congruent modulo m if and only if they have the same remainders when they are divided by m .

Proof in one direction:

If $a \bmod m = b \bmod m$, then $a = q_1m + r$ and $b = q_2m + r$ for some integers q_1, q_2, r .

Then $a - b = (q_1 - q_2)m$. That means that m divides $a - b$, which is the definition of $a \equiv b \pmod{m}$.

Congruence Theorems

$$a \equiv a \pmod{m} \quad \text{Reflexive}$$

$$\text{If } a \equiv b \pmod{m} \text{ then } b \equiv a \pmod{m} \quad \text{Symmetric}$$

$$\text{If } a \equiv b \pmod{m} \text{ and } b \equiv c \pmod{m}, \text{ then } a \equiv c \pmod{m} \quad \text{Transitive}$$

$$a \equiv b \pmod{m} \text{ if and only if } a + k \equiv b + k \pmod{m}$$

$$\text{If } a \equiv b \pmod{m}, \text{ then } ak \equiv bk \pmod{m}$$

$$\text{If } a \equiv b \pmod{m} \text{ and } c \equiv d \pmod{m}, \text{ then } a + c \equiv b + d \pmod{m}$$

Proofs with Quantifiers

Existentials: sometimes we need to show that there is an object with a certain property such that something is true.

We can often do this by construction. We find an object that has the property by trial and error, or give an algorithm for producing it. We have to be sure that the object has the property and that the "something" is true.

Show that there is an integer n that can be written in two ways as the sum of two primes.

Proofs with Quantifiers

Existentials: sometimes we need to show that there is an object with a certain property such that something is true.

We can often do this by construction. We find an object that has the property by trial and error, or give an algorithm for producing it. We have to be sure that the object has the property and that the "something" is true.

Show that there is an integer n that can be written in two ways as the sum of two primes.

$$30 = 13 + 17 = 11 + 19$$

Proofs with Quantifiers

Theorem: There exists a unique prime number of the form $n^2 - 1$ where n is an integer ≥ 2 .

Existence Proof: The prime number $3 = 2^2 - 1$.

Uniqueness Proof: Suppose that $m > 2$ and $m^2 - 1$ is prime. Then $(m - 1)(m + 1)$ is prime. But $m - 1$ and $m + 1$ are both greater than 1, so $m^2 - 1$ is not prime. This is a contradiction, so no such m exists.