CHAPTER 4

Number Theory

4.1 Divisibility and Modular Arithmetic

4.5 Applications of Congruences

4.3 Primes and Greatest Common Divisors

4.2 Integer Representations and Algorithms

4.3 Primes and Greatest Common Divisors

Primes

prime factorization

The Sieve of Eratosthenes

4.3 Primes and Greatest Common Divisors

Primes

An integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called *composite*.

the integer 9 is composite

p	d	r

The integer 7 is prime

p	d	r

```
bool isprime(p)
{ if(p<=1)
      return false;
  d = 2;
  while(p%d ≠ 0)
      d = d+1;
  if(d<p) return f;
  return true;
}
```

4.3 Primes and Greatest Common Divisors

Primes

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

```
bool isprime(p)
{ if(p<=1)
     return false;
  d=2;
  while(p%d≠0)
     d=d+1;
  if(d<p) return f;
  return true;
}
```

Show that 101 is prime.

p	d	r

p	d	r

Show that 101 is prime.

p	d	r

THE FUNDAMENTAL THEOREM OF ARITHMETIC Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

```
        prime
void    factorization (int n)
{ p=2;
  while (n>1)
    if (n%p==0)
    {         p ;
      n = n/p;
    } else  p++;
```

n | p | n mod p
500 | 2 |

4.3 Primes and Greatest Common Divisors

Greatest Common Divisors

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

What is the greatest common divisor of 24 and 36?

What is the greatest common divisor of 17 and 22?

The integers a and b are *relatively prime* if their greatest common divisor is 1.

Greatest Common Divisors

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n},\ b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)},$$

$120 = 2^3 \cdot 3 \cdot 5$ $\quad$ $500 = 2^2 \cdot 5^3$

$$\gcd(120, 500) = 2^{\min(3, 2)} 3^{\min(1, 0)} 5^{\min(1, 3)} = 2^2 3^0 5^1 = 20.$$

4.3 Primes and Greatest Common Divisors

least common multiple

The *least common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $\operatorname{lcm}(a, b)$.

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

$$\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)},$$

$120 = 2^3 \cdot 3 \cdot 5 \qquad 500 = 2^2 \cdot 5^3$

What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

$$\gcd(120, 500) = 2^{\min(3,2)} 3^{\min(1,0)} 5^{\min(1,3)} = 2^2 3^0 5^1 = 20.$$

Let a and b be positive integers. Then

$$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b).$$

The Euclidean Algorithm

Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

$$287 = 91 \cdot 3 + 14.$$

$$91 = 14 \cdot 6 + 7.$$

$$14 = 7 \cdot 2.$$

x	y	r	q
287	91		

The Euclidean Algorithm.

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return $x\{\gcd(a, b)$ is $x\}$

The Sieve of Eratosthenes

4.3 Primes and Greatest Common Divisors

is used to find all primes not exceeding a specified positive integer.

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	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

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	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

4.3 Primes and Greatest Common Divisors

THE INFINITUDE OF PRIMES

There are infinitely many primes.

Proof:

$p_1, p_2, \ldots, p_n$

$Q = p_1 p_2 \cdots p_n + 1.$

THE FUNDAMENTAL THEOREM OF ARITHMETIC

Q is a composite

if $p_j \mid Q$, then p_j divides $Q - p_1 p_2 \cdots p_n = 1.$

p_j is not a prime.

Q has a prime factor that is not in the set {p1, p2, .., pn}.

THE PRIME NUMBER THEOREM

The number of primes not exceeding x is $x/\ln x$.

Conjectures and Open Problems About Primes