

C H A P T E R

4

Number Theory

4.1 Divisibility and
Modular
Arithmetic

4.5 Applications of
Congruences

4.3 Primes and
Greatest
Common
Divisors

4.2 Integer Repre-
sentations and
Algorithms

4.3

Primes and Greatest Common Divisors

Primes

prime factorization

The Sieve of Eratosthenes

4.3

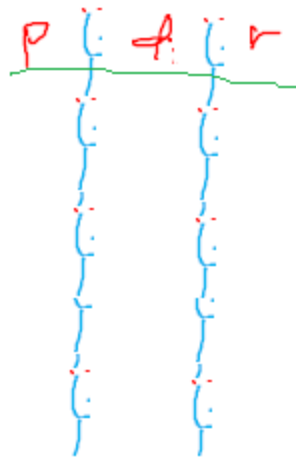
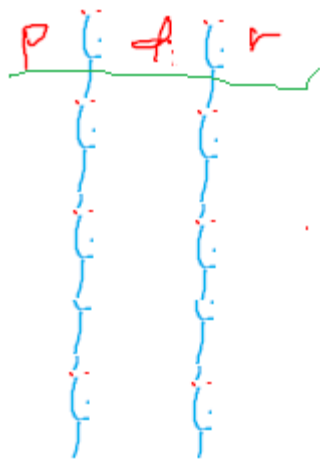
Primes and Greatest Common Divisors

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

The integer 7 is prime



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

4.3

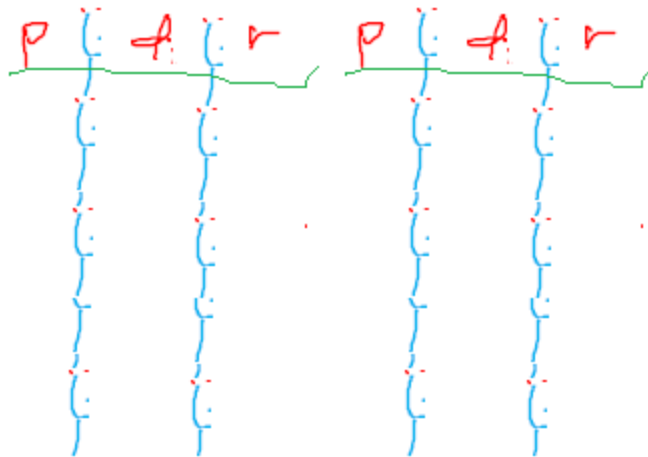
Primes and Greatest Common Divisors

Primes

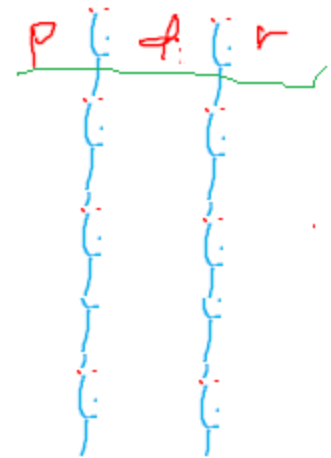
If n is a composite integer, then n has a prime divisor less than or equal to \sqrt{n} .

```
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.



Show that 101 is prime.



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++;
    }
}
    
```

$$\frac{n}{500} \mid \frac{p}{2} \mid \frac{n \bmod p}{}$$

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

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

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

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

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

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

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 $\text{lcm}(a, b)$.

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

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

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

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

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

Let a and b be positive integers. Then

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

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  $y \neq 0$ 
     $r := x \bmod y$ 
     $x := y$ 
     $y := r$ 
return  $x$  {gcd( $a, b$ ) is  $x$ }
    
```

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

1	2	3	<u>4</u>	5	<u>6</u>	7	<u>8</u>	9	<u>10</u>
11	<u>12</u>	13	<u>14</u>	15	<u>16</u>	17	<u>18</u>	19	<u>20</u>
21	<u>22</u>	23	<u>24</u>	25	<u>26</u>	27	<u>28</u>	29	<u>30</u>
31	<u>32</u>	33	<u>34</u>	35	<u>36</u>	37	<u>38</u>	39	<u>40</u>
41	<u>42</u>	43	<u>44</u>	45	<u>46</u>	47	<u>48</u>	49	<u>50</u>
51	<u>52</u>	53	<u>54</u>	55	<u>56</u>	57	<u>58</u>	59	<u>60</u>
61	<u>62</u>	63	<u>64</u>	65	<u>66</u>	67	<u>68</u>	69	<u>70</u>
71	<u>72</u>	73	<u>74</u>	75	<u>76</u>	77	<u>78</u>	79	<u>80</u>
81	<u>82</u>	83	<u>84</u>	85	<u>86</u>	87	<u>88</u>	89	<u>90</u>
91	<u>92</u>	93	<u>94</u>	95	<u>96</u>	97	<u>98</u>	99	<u>100</u>

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

1	2	3	<u>4</u>	5	<u>6</u>	7	<u>8</u>	<u>9</u>	<u>10</u>
11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>
<u>21</u>	<u>22</u>	23	<u>24</u>	<u>25</u>	<u>26</u>	<u>27</u>	<u>28</u>	29	<u>30</u>
31	<u>32</u>	<u>33</u>	<u>34</u>	<u>35</u>	<u>36</u>	37	<u>38</u>	<u>39</u>	<u>40</u>
41	<u>42</u>	43	<u>44</u>	<u>45</u>	<u>46</u>	47	<u>48</u>	<u>49</u>	<u>50</u>
<u>51</u>	<u>52</u>	53	<u>54</u>	<u>55</u>	<u>56</u>	<u>57</u>	<u>58</u>	59	<u>60</u>
61	<u>62</u>	<u>63</u>	<u>64</u>	<u>65</u>	<u>66</u>	67	<u>68</u>	<u>69</u>	<u>70</u>
71	<u>72</u>	73	<u>74</u>	<u>75</u>	<u>76</u>	<u>77</u>	<u>78</u>	79	<u>80</u>
<u>81</u>	<u>82</u>	83	<u>84</u>	<u>85</u>	<u>86</u>	<u>87</u>	<u>88</u>	89	<u>90</u>
<u>91</u>	<u>92</u>	<u>93</u>	<u>94</u>	<u>95</u>	<u>96</u>	97	<u>98</u>	<u>99</u>	<u>100</u>

4.3

Primes and Greatest Common Divisors

THE INFINITUDE OF PRIMES

There are infinitely many primes.

Proof:

$$p_1, p_2, \dots, p_n$$

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

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 $\{p_1, p_2, \dots, p_n\}$.

THE PRIME NUMBER THEOREM

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

Conjectures

and

Open Problems

About Primes