

8. Prime Numbers

We know that any integer a greater than 1 has the positive divisors 1 and a . Many have more than two divisors. Positive divisors other than 1 and a are sometimes called *proper divisors* or *proper factors* of a . Note that the proper divisors, if any, lie between 1 and a .

Definition

An integer $p > 1$ is a *prime number* if it has *exactly* two divisors.

An integer $p > 1$ is a *composite number* if it is *not* a prime number.

Note. The integer 1 is regarded as *neither* prime *nor* composite.

The first few primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31,

Theorem 1

If n is composite, then it has a divisor w with $1 < w \leq \sqrt{n}$.

Proof

As n is composite, it has a proper divisor u .

As u is a divisor of n , $n = uv$ for some integer v .

As u is proper, $1 < u < n$, so that $1 < v < n$, so v is also a proper divisor of n

If u and v are *both* greater than \sqrt{n} , then $uv > n$.

This is a contradiction as $uv = n$.

Thus, one of u, v is less than \sqrt{n} . We may choose this as w .

Corollary

If the integer $n > 1$ has no divisor w in the range $1 < w \leq \sqrt{n}$, then n is prime.

This speeds up the process of identifying primes. For example $\sqrt{97} = 9.848\dots$

If 97 were composite, the Corollary would imply a divisor in the range 2, ..., 9.

It is easy to check that none is a divisor. Thus 97 is prime.

Example Show that every prime greater than 2 is of the form $4K+1$ or $4K-1$.

Solution

We know that every integer n has one of the forms $4k, 4k+1, 4k+2, 4k+3$.

Numbers of the forms $4k$ and $4k+2$, other than 2, have a proper factor 2.

It follows that such numbers are composite so a prime must be $4k+1$ or $4k+3$.

The latter can be rewritten $4K-1$, with $K = k-1$.

Example Show that every prime greater than 3 is of the form $6K+1$ or $6K-1$.

Solution

We know that every integer has one of the forms $6K+r$, with $0 \leq r < 6$.
Other than 2, each integer of the form $6K$, $6K+2$ or $6K+4$ has a proper factor 2.
Other than 3, each integer of the form $6K$ or $6K+3$ has a proper factor 3.
Thus, any prime other than 2, 3 has one of the forms $6K+1$, $6K+5$.
Numbers of the latter type can be rewritten as $6L-1$, where $L = K+1$.

The next theorem refers to a *product of primes*. This is an integer of the form $N = p(1).p(2)....p(r)$, where $(p(1), p(2),....., p(r))$ is a *list* of prime numbers.

Notes

1. There is *no* requirement that the $p(i)$ are distinct. For example, 24 is the product of (the list of) primes (2, 2, 2, 3).
2. If the “list” consists of a *single* prime p , the “product” is just p itself.
3. If the integers M, N are products of primes, then MN is a product of primes. A suitable list for MN is the combination of the lists for M and N .

Theorem 2 Every integer greater than 1 is a product of primes.

Proof

Assumption : Suppose that the result is *false*.

Then there is a *smallest* integer $n > 1$ which is *not* a product of primes.

This n is *not* prime, since each prime *is* a product of primes, by Note (2) above.

Hence, n is composite, so that $n = uv$, where u, v are integers with $1 < u, v < n$.

Now $u, v < n$, and n is the smallest integer which is *not* a product of primes.

Thus each of u, v is a product of primes.

Then, by Note (3), $n = uv$ is a product of primes.

Thus n is **and** is *not* a product of primes - a contradiction.

Our *assumption* must be false – i.e. the theorem is actually true.

Corollary Every integer greater than 1 has a factor which is prime.

Proof If $n > 1$, Theorem 2 shows that n is a product of primes. Clearly, each of the primes in the list for n is a factor of n .

The next result is one of the classic theorems of mathematics. It is frequently attributed to Euclid. It certainly appears in his book on Number Theory.

Note. You may be asked for a proof in a 2N examination.

Lemma If $n > 1$ and n divides m , then n does *not* divide $m+1$.

Proof

As $n \mid m$, $m = nk$, for some integer k

Then $m+1 = nk+1$, so $m+1$ has remainder 1 on division by n .

This means that n does *not* divide $m+1$ (otherwise the remainder would be 0).

Theorem 3 - Euclid's Theorem There are infinitely many prime numbers

Proof - EXAMINABLE

Assumption : Suppose that the result is *false*.

Then there is only a *finite* set $\mathbf{S} = \{p(1), \dots, p(r)\}$ of primes.

Let $m = p(1).p(2)...p(r)$ – note that it follows that each $p(i)$ divides m .

By the above Corollary, $m+1$ has a prime factor p . (1)

But, by our assumption, every prime lies in \mathbf{S} , so $p = p(i)$ for some i .

But $p(i)$ divides m , so, by the Lemma, it does *not* divide $m+1$. (2)

Thus, $p(i)$ divides $m+1$, by (1), and *does not divide* $m+1$, by (2)

This contradiction shows that our *assumption* is false, so the *theorem* is true.

Example Suppose that p is a prime.

Show that, for any integer a , $\gcd(a,p)$ is always 1 or p

Determine the integers a for which $\gcd(a,p) = p$.

Solution

Let $d = \gcd(a,p)$. Then we know that $d \mid p$.

As p is prime, its only positive divisors are 1 and p .

Thus d must be 1 or p .

The gcd is p precisely when p also divides a .

Theorem 4

Let p be a prime, and $a, b \in \mathbf{N}$. If $p \mid ab$, and $p \nmid a$, then $p \mid b$.

Proof

From the above example, $\gcd(a,p) = 1$ or p . As $p \nmid a$, we have $\gcd(a,p) = 1$. The result follows by Euclid's Lemma.

The result may be restated as "if $p \mid ab$, then $p \mid a$ or $p \mid b$ ". It is then easily generalized to :

Corollary 4a Suppose that p is prime, and that $a(1), \dots, a(r)$ are integers. If $p \mid a(1) \dots a(r)$, then $p \mid a(i)$ for some i .

Theorem 5 – The Fundamental Theorem of Arithmetic

Each integer $n > 1$ can be expressed as a product of primes. The product is *unique*, apart from the order of the factors.

Proof

The first part is just a restatement of Theorem 2.

We now know that each n has *at least one* expression as a product of primes.

Assumption : the Theorem is *false*.

For the Theorem to be false, there must be integers with two expressions.

Let n be the *smallest* integer with two expressions. Say

$$n = p(1) \dots p(t) = q(1) \dots q(s) \quad (1),$$

where the $p(i)$ and $q(j)$ are prime.

Now $p(1)$ divides $n = p(1) \dots p(t)$, so that it also divides $q(1) \dots q(s)$.

By Corollary 4a, as $p(1)$ is prime, and divides $q(1) \dots q(s)$, we must have $p(1) \mid q(i)$ for some integer i .

But $q(i)$ is prime, so we must have $p(1) = q(i)$.

We now divide each part of (1) by $p(1)$. In the last part, this simply deletes the factor $q(i)$ since this is equal to $p(1)$.

We thus have integer $m = p(2) \dots p(t)$ with two expressions as a product of primes.

But $m < n$, and n was chosen as the *smallest* integer with two expressions.

This is a contradiction – the Theorem must be true.

In the factorisation of n , a given prime p may occur more than once. Suppose that the *distinct* prime factors of n are $p(1), \dots, p(r)$, and that, for each i , the factor $p(i)$ occurs $a(i)$ times. Then we can write

$$n = p(1)^{a(1)} \dots p(r)^{a(r)} = \prod_{i=1}^r p(i)^{a(i)}$$

It is sometimes convenient to allow $a(i) = 0$, indicating that $p(i)$ is *not* a factor in n . If we put *all* of the $p(i)$ equal to 0, we get an expression for the integer $n = 1$.

Note. Any factor m of the integer n with this expression must have the form

$$m = \prod_{i=1}^r p(i)^{c(i)}$$

with $0 \leq c(i) \leq a(i)$ for each i .

The expression of integers as products of primes leads to some useful results. We will state two of these without proof.

Suppose that

$$n = \prod_{i=1}^r p(i)^{a(i)} \quad \text{and} \quad m = \prod_{i=1}^r p(i)^{b(i)}$$

Fact 1 $m \mid n$ if and only if $b(j) \leq a(j)$ for each j .

Example

Since $15 = 3^1 \cdot 5^1$, the divisors of 15 are

$$3^0 \cdot 5^0 = 1, \quad 3^1 \cdot 5^0 = 3, \quad 3^0 \cdot 5^1 = 5 \quad \text{and} \quad 3^1 \cdot 5^1 = 15.$$

Fact 2

$$\gcd(n, m) = \prod_{i=1}^r p(i)^{c(i)} \quad \text{and} \quad \text{lcm}(n, m) = \prod_{i=1}^r p(i)^{d(i)}$$

where $c(j) = \min(a(j), b(j))$, and $d(j) = \max(a(j), b(j))$.

Example

For $n = 12$, $m = 15$, we have $12 = 2^2 \cdot 3^1 \cdot 5^0$ and $15 = 2^0 \cdot 3^1 \cdot 5^1$.

Then $\gcd(12, 15) = 2^0 \cdot 3^1 \cdot 5^0 = 3$, and $\text{lcm}(12, 15) = 2^2 \cdot 3^1 \cdot 5^1 = 60$

Fact 3

The number of positive divisors of $n \in \mathbb{N}$ is denoted by $\tau(n)$ (read tau of n). Then $\tau(n) = (a(1)+1).(a(2)+1).(a(r)+1)$, where n is given by

$$n = \prod_{i=1}^r p(i)^{a(i)}$$

For example, $\tau(15) = 2.2 = 4$ since $15 = 3^1.5^1$.

Proof of Fact 3

From Fact 1, we know that any divisor m of n can be written as

$$m = \prod_{i=1}^r p(i)^{b(i)}$$

with $0 \leq b(j) \leq a(j)$.

Thus, for a given j , there are $a(j)+1$ possible values of $b(j)$.

So, $b(1)$ can be chosen in $a(1)+1$ ways, ..., $b(r)$ can be chosen in $a(r)+1$ ways.

Thus m can be chosen in $(a(1)+1).(a(2)+1).(a(r)+1)$ ways.

Prime decomposition

We first showed that any integer n greater than 1 can be written as a product of primes. The expression is unique, *apart from the order of the prime factors*. We then grouped together any repeated factors. This allowed us to write

$$n = \prod_{i=1}^r p(i)^{a(i)}$$

Provided that we do not include terms with $a(j) = 0$, this product is unique *up to the order of the primes*.

As the $p(j)$ are *distinct*, we can order the primes so that $p(1) < p(2) < \dots < p(r)$.

Once this choice is made, the expression for n is unique.

We refer to it as the *prime decomposition* of n .

Example

Find the prime decomposition of 120

Solution

When we express 120 as a product of primes, the product has factors 2,2,2,3,5.

Thus the prime decomposition of 120 is $2^3 \cdot 3^1 \cdot 5^1$.

Also, $\tau(120) = (3+1)(1+1)(1+1) = 4 \cdot 2 \cdot 2 = 16$, so

120 has 16 positive divisors.

Exercise to reader

1. Find the prime decomposition of 60.
2. Determine $\tau(60)$, the number of positive divisors of 60.
3. Write down all the positive divisors of 60.

Hint. For (3), look at the proof of Fact 3.