CHAPTER 1

# Theory of Numbers

*In this section, we discuss properties peculiar to whole numbers. The word 'number' is taken to mean 'whole number', and, unless otherwise stated, 'positive whole number.'*

## 1. Division:

**(1)** Let $b$ be any positive whole number, and consider the sequence

$$\ldots -3b, -2b, -b, 0, b, 2b, 3b, \ldots$$

continued indefinitely both ways. Any whole number $a$ (positive, negative or zero) is either a term of this sequence, or it lies between two consecutive terms. Thus two numbers $q$ and $r$ can be determined uniquely so that

$$a = bq + r \text{ and } 0 \leq r < b. \qquad \ldots(A)$$

To *divide* $a$ by $b$ is to find the numbers $q$ and $r$ which satisfy these conditions; $q$ is called the *quotient* and $r$ the *remainder.*

If $r = 0$, we say that $a$ is *divisible* by $b$ or is a *multiple* of $b$, and that $b$ is a *divisor* or a *factor* of $a$. Among the divisors of a number we count the number itself and 1.

Whatever $b$ may be, $0 = b \cdot 0 + 0$; hence zero must be regarded as divisible by every whole number.

**(2)** If $r = b - r'$, we have

$$a = b(q + 1) - r' \quad \text{and} \quad 0 \leq r' < b;$$

also if $r \geq \frac{1}{2} b$ then $r' \leq \frac{1}{2} b$. Hence it is always possible to find numbers $Q$ and $R$ such that

$$a = bQ + R \quad \text{and} \quad |R| \leq \frac{1}{2} b.$$

**Example 1.** *Every number is of one of the forms $5n$, $5n \pm 1$, $5n \pm 2$.*

For if any number is divided by 5, the remainder is one of numbers 0, 1, 2, 5 – 2, 5 – 1.

**Example 2.** *Every square number is of one of the forms $5n$, $5n \pm 1$.*

The square of every number is of one of the forms $(5m)^2$, $(5m \pm 1)^2$, $(5m \pm 2)^2$. If these are divided by 5, the remainders are 0, 1, 4; and, since $4 = 5 - 1$, the forms are $5n$, $5n + 1$, and $5n - 1$.

**Example 3.** *The square of every odd number is of the form 8n + 1.*

For $(2k + 1)^2 = 4k\ (k + 1) + 1$, and either $k$ or $k + 1$ must be even, so that $k\ (k + 1)$ is divisible by 2.

### 2. Theorems on Division:

**(1)** *If both a and b are divisible by c, so also is ma ± nb.*

**(2)** *If r is the remainder when a is divided by b, then cr is the remainder when ca is divided by cb.*

For if $a = bq + r$ and $0 \le r < b$,

then $ca = (cb)q + cr$ and $0 \le cr < cb$.

**(3)** *If both a and b are divisible by c, and r is the remainder when a is divided by b, then* (*i*) *r is divisible by c and* (*ii*) *r/c is the remainder when a/c is divided by b/c.*

For if $a = bq + r$ and $0 \le r < b$, then since $a$ and $b$ are divisible by $c$, so also is $r$, which is equal to $a - bq$. Thus we have

$$a/c = (b/c)q + r/c \text{ where } 0 \le r/c < b/c.$$

### 3. Theorems on the Greatest Common Divisor:

**(1)** *If r is the remainder when a is divided by b, the common divisors of a and b are the same as those of b and r.*

For, since $a = bq + r$, every common divisor of $b$ and $r$ is a divisor of $a$; and, since $r = a - bq$, every common divisor of $a$ and $b$ is a divisor of $r$. This proves the statement in question.

**(2)** *If a and b are any two numbers, there exists a number g, and one only, such that the common divisors of a and b are the same as the divisors of g.*

For numbers $(q_1, r_1), (q_2, r_2)$, etc., can always be found in succession, and uniquely, so that

$$a = bq_1 + r_1,\ b = r_1q_2 + r_2,\quad r_1 = r_2q_3 + r_3, \text{ etc.,} \qquad ...(A)$$

where $b > r_1 > r_2 > r_3 \ldots \ge 0$.

Since the number of positive integers less than $b$ is limited, a zero remainder must occur; and, supposing that $r_{n+1} = 0$, the process terminates with

$$r_{n-2} = r_{n-1}q_n + r_n,\ r_{n-1} = r_nq_{n+1}.$$

Hence, by (A), the following pairs of numbers have the same common divisors:

$$(a, b)\ (b, r_1), (r_1, r_2), \ldots, (r_{n-1}, r_n);$$

and, since $r_{n-1} = r_nq_{n+1}$, the common divisors of $r_{n-1}$ and $r_n$ are the divisors of $r_n$. Hence the number $g$ exists, and its value is $r_n$.

Since $g$ is divisible by any common divisor of $a$ and $b$, it is the *greatest common divisor* of these numbers and is known in elementary arithmetic as the greatest common measure (G.C.M.) of $a$ and $b$.*

**(3)** *If a and b are each multiplied by any number m, or are divided by a common divisor m, then g, the greatest common divisor of a and b, is multiplied or divided by m.*

For each of the *r's* in the proof of (2) is multiplied or divided by $m$.

**(4)** If *a, b, c,* ..., are serveral numbers, and $g_1$ is the greatest common divisor of $a$ and $b$, $g_2$ that of $g_1$ and $c$, $g_3$ that fo $g_2$ and $d$, and so on, then the following sets of

* The process, here stated algebraically, is that used in Elementary Arithmetic.

numbers have the same common divisors:

$$(a, b, c, d, \ldots), (g_1, b, c, d, \ldots), (g_2, c, d, \ldots), \text{ etc.}$$

Hence we arrive eventually at a number $g$, whose divisors are the common divisors of $a, b, c, \ldots$; also $g$ is uniquely determined. This number $g$ is the *greatest common divisor*, or the *greatest common measure* of $a, b, c, \ldots$ .

■ **4. Numbers Prime to each other:** Two numbers, $a$ and $b$, are said to be prime to each other when their greatest common divisor is 1, so that they have no common divisor except 1. This is often expressed by saying that $a$ is prime to $b$, or that $b$ is prime to $a$. The following theorems are fundamental.

**(1)** *If the product ab is divisible by a number m, and m is prime to one factor a, then m is a divisor of the other factor b.*

For, if $a$ is prime to $m$, the greatest common divisor of $a$ and $m$ is 1; hence the greatest common divisor of $ab$ and $mb$ is $b$. But, by hypothesis, $m$ is a divisor of $ab$, and is therefore a common divisor of $ab$ and $mb$; hence $m$ is equal to, or is a divisor of, $b$.

**(2)** *If a is prime to b, and each of these numbers is a divisor of N, then ab is a divisor of N.*

Suppose that $N = aq$, then $b$ is a divisor of $aq$, and since $b$ is prime to one factor $a$, it must be a divisor of the other factor $q$. Let $q = mb$, then $N = mab$, and $ab$ is a divisor of $N$.

**(3)** *If a is prime to b, positive integers x, y can be found such that*

$$ax - by = \pm 1.$$

For it follows from equations (A) of Art. 3, (2), that

$$r_1 = a - bq_1,\ r_2 = -aq_2 + b\,(1 + q_1q_2),$$
$$r_3 = a\,(1 + q_2\,q_3) - b\,(q_1 + q_3 + q_1q_2q_3).$$

Continuing thus, *every remainder can be expressed in the form* $\pm (ax - by)$, *where x, y are positive integers.*

If $a$ is prime to $b$, the last remainder is 1, and the theorem follows.

■ **5. Theorems on Prime Numbers:** A number which has no divisors except itself and 1 is called a *prime number*, or simply a *prime.* Numbers which are not prime are said to be *composite.*

**(1)** *A prime number, p, is prime to every number which is not a multiple of p.*

For, if $a$ is any such number, $q$ and $r$ can be found such that $a = pq + r$ where $0 < r < p$. Now $p$ and 1 are the only divisors of $p$, and as $r < p$, the only common divisor of $p$ and $r$ is 1, that is to say, $p$ is prime to $r$ and therefore to $a$.

**(2)** *If a prime p is a divisor of a product abcd ... hk, it is a divisor of at least one of the factors a, b, .... k.*

For if the prime $p$ is not a divisor of $a$, by Theorem (1) it is prime to $a$, hence it is a divisor of $bcd \ldots k$. If, in addition, $p$ is not a divisor of $b$, it must be a divisor of $cd \ldots k$. Continuing thus, it can be shown that if $p$ is not a divisor of any of the numbers $a, b, c, \ldots h$, it must be a divisor of $k$.

■ **6. Theorems on Numbers, Prime or Composite:**

**(1)** *Every composite number N has at least one prime divisor.*

For, since $N$ is not a prime, it has a divisor, $n$, different from $N$ and from 1, which is *not greater than any other divisor.* Further, this divisor must be a prime; for, otherwise, it would have a divisor *less* than itself and greater than 1, and this latter would be a divisor of $N$. This contradicts the hypothesis that $n$ is not greater than any other divisor.

It follows that every composite number, $N$, can be expressed as the product of prime factors.

For, since $N$ has at least one prime factor, $p$, we have $N = pa$, where $1 < p < N$. If $a$ is not a prime, it has at least one prime factor, $q$; and $a = qb$, where $1 < b < a$.

Thus, $N = pa = pqb$ ; and so on.

But the numbers less than $N$ are limited; and $N > a > b > ...$, therefore the set $N, a, b, ...$ must finally end in a prime. Hence, $N$ can be expressed in the form, $N = pqr ... u$, where $p,q,r, ..., u$ are all primes, not necessarily all different.

That is to say, any composite number, $N$, can be expressed as

$$N = p^a.q^b.r^c ... u^s,$$

where $p, q, r, ... , u$ are all different primes.

**(2)** *A composite number can be expressed as the product of prime factors in one way only.*

For suppose that $N = p^aq^br^c ....= P^AQ^BR^C ...$ where $p, q, r, ..., P, Q, R, ...,$ are primes; then, since the prime $P$ is a divisor of the product $p^aq^br^c ...$, it is a divisor of one of the factors $p, q, r, ...$ , and is therefore equal to one of them. In the same way each of the set $P, Q, R, ...$ is equal to one of the set $p, q, r, ...$ , and no prime factor can occur in one of the expressions for $N$ which does not occur in the other. Suppose then that

$$N = p^aq^br^c ... = p^Aq^Br^C ... .$$

If $a \neq A$, one of them must be the greater. Let $A > a$, and suppose that $A = a + e$, then $q^b . r^c. ... t^m = p^e. q^B. r^C. ... t^M$ ; but this is impossible, as the left-hand side of the equality is a number prime to $p$, and the right-hand side is divisible by $p$.

Hence, $a$ must be equal to $A$; and similarly, $b = B, ..., m = M$ ; and thus the two expressions for $N$ are identical.

The above theorem is one of the most important in the Theory of Numbers, and the following propositions are immediately deducible.

**(3)** *If m is prime to each of the numbers, a b, ..., k, it is prime to the product ab ... k.*

**(4)** *If a is prime to b, then $a^n$ is prime to $b^n$, where n is any integer; and conversely.*

**(5)** *A number N is a prime, if it is not divisible by any prime number greater than* 1 *and less than, or equal to,* $\sqrt{N}$.

For, if $N = ab$, where $b \geq a$, *then* $N \geq a^2$; that is, $a \leq \sqrt{N}$ .

**(6)** *The sequence of primes is endless.*

For, if $p$ is any prime, the number $\lfloor p + 1$ is greater than $p$ and is not divisible by $p$ or by any smaller prime. If then $\lfloor p + 1$ is not a prime, it must have a prime divisor greater than $p$, and in either case a prime greater than $p$ exists.

All the primes less than a given number $N$ can be obtained in order by a process called the *Sieve of Eratosthenes.* The process consists in writing down in order all the numbers from 1 to $N - 1$, and erasing all multiples of the primes 2, 3, 5, 7, ... which

are less than $\sqrt{N}$ . Nevertheless, the problem of discovering whether a large number is prime or composite is one of great difficulty.

**Example 1.** *If n is any number, prove that n(n + 1) (n + 2) is divisible by 6.*

Of the two consecutive numbers, $n$ and $n + 1$, one is divisible by 2; and one of the three consecutive numbers, $n$, $n + 1$, $n + 2$, is divisible by 3. Hence the product $n\ (n + 1)\ (n + 2)$ is divisible by 2 and by 3; and, since 2 is prime to 3, $n\ (n + 1)\ (n + 2)$ is divisible by 6.

**Example 2.** *Prove that* $3^{2n+1} + 2^{n+2}$ *is divisible by 7.*

We have $3^{2n+1} = 3.\ 9^n = 3\ (7 + 2)^n = 7k + 3\ .\ 2^n$, by the Binomial theorem,

and $2^{n+2} = 4\ .\ 2^n$;

$\therefore \quad 3^{2n+1} + 2^{n+2} = 7k + 2^n\ (3 + 4) = 7\ (k + 2^n)$.

**7. The Divisors of a Given Number N:** *Let* $N = p^a\ .\ q^b\ .\ r^c\ .\ ...$, *where p, q, r, ....., are primes; and let n be the number, and s the sum, of the divisors of N, including* 1 *and N.*

*Then,* **(1)**
$$n = (a + 1)\ (b + 1)\ (c + 1)\ ....;$$
$$s = \frac{p^{a+1} - 1}{p - 1} \cdot \frac{q^{b+1} - 1}{q - 1} \cdot \frac{r^{c+1} - 1}{r - 1} \cdot ... \cdot$$

For the divisors of $N$ are the terms in the expansion of

$$(1 + p + p^2 + ... + p^a)\ (1 + q + q^2 + ... + q^b)\ (1 + r + r^2 + ... + r^c)\ ... ;$$

and the expressions for $n$ and $s$ follow immediately.

**(2)** *The number of ways in which N can be expressed as the product of two factors, including N and 1, is* $\frac{1}{2}\ (n + 1)$ *or* $\frac{1}{2}\ n$, *according as N is, or is not, a perfect square.*

For, if $N$ is a perfect square, each of the numbers, $a, b, c, ...$, is even, and therefore $n$ is odd; but if $N$ is not a perfect square, at least one of these numbers is odd, and therefore $n$ is even.

Further, if $d_1\ (= 1), d_2, d_3, ..., d_{n-2}, d_{n-1}, d_n\ (= N)$, are the divisors of $N$ in ascending order, the different ways of expressing $N$ as the product of two factors are:

$d_1\ d_n,\ d_2 d_{n-1},\ d_3 d_{n-2},\ ...,\ d_x d_x,$ when $n = 2x - 1$,

and $d_1 d_n,\ d_2 d_{n-1},\ d_3 d_{n-2},\ ...,\ d_y d_{y+1},$ when $n = 2y$.

Hence, the number of ways is either $x$ or $y$; *i.e.* either $\frac{1}{2}\ (n + 1)$ or $\frac{1}{2}\ n$, according as $N$ is, *or* is not, a perfect square.

**(3)** *The number of ways in which N can be expressed as the product of two factors, which are prime to one another, is* $2^{m-1}$, *where m is the number of different prime factors of N.*

For, such factors are the terms in the expansion of

$$(1 + p^a)\ (1 + q^b)\ (1 + r^c)\ ... ;$$

and their number is $2^m$. Hence the number of pairs is $2^{m-1}$.

For example, if $N = 2^2\ .\ 3^3\ .\ 5 = 540$, $n = (2 + 1)\ (3 + 1)\ (1 + 1) = 24$,

$$s = \frac{2^3 - 1}{2 - 1} \cdot \frac{3^4 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 1680, \text{ and } m = 3,\ 2^{m-1} = 4.$$

■ **8. The Symbol I [*x*/*y*]:** If $a$ is a fraction or an irrational number, the symbol $I(a)$ will be used to denote the integral part of $a$. Thus if $x = qy + r$ where $0 \leq r < y$, then $I(x/y) = q$.

**(1)** *If $n_1, n_2, n_3, \ldots$, are any integers, and s is their sum and a is any number, then*

$$I[s/a] \geq I[n_1/a] + I[n_2/a] + I[n_3/a] + \ldots .$$

Let $n_1 = aq_1 + r_1$, $n_2 = aq_2 + r_2$, $n_3 = aq_3 + r_3$, etc.; then

$$s = a(q_1 + q_2 + q_3 + \ldots) + (r_1 + r_2 + r_3 + \ldots).$$

Hence, $I[s/a] = (q_1 + q_2 + q_3 + \ldots) + I[(r_1 + r_2 + r_3 + \ldots)/a]$;

and, since $q_1 = I[n_1/a]$, $q_2 = I[n_2/a]$,... , the result follows.

**(2)** *The highest power of a prime p which is contained in $\lfloor\underline{n}$ is*

$$I[n/p] + I[n/p^2] + I[n/p^3] + \ldots .$$

For, of the numbers from 1 to $n$ inclusive, there are $I[n/p]$ which are divisible by $p$; of these $I[n/p^2]$ are divisible by $p^2$ ; and so on; hence the result follows.

■ **9. Theorems:**

**(1)** *The product of any n consecutive integers is divisible by $\lfloor\underline{n}$ .*

For $(m + 1)(m + 2) \ldots (m + n)/\lfloor\underline{n} = \lfloor\underline{m+n}/\lfloor\underline{m}\lfloor\underline{n}$, and to show that the last expression is an integer it is sufficient to show that any prime $p$ which occurs in $\lfloor\underline{m}\lfloor\underline{n}$ occurs to at least as high a power in $\lfloor\underline{m+n}$. Thus we have to show that

$$I[(m + n)/p] + I[(m + n)/p^2] + I[(m + n)/p^3] + \ldots$$
$$\geq I[m/p] + I[m/p^2] + I[m/p^3] + \ldots$$
$$+ I[n/p] + I[n/p^2] + I[n/p^3] + \ldots .$$

Now $I[(m + n)/p] \geq I[m/p] + I[n/p]$, and the same is true if we replace $p$ by $p^2$, $p^3$, ..., in succession: hence the result in question.

**(2)** *If n is a prime, $C_r^n$ is divisible by n.*

For by the preceding $n(n-1)(n-2) \ldots (n-r+1)$ is divisible by $\lfloor\underline{r}$, and since $n$ is a prime and $r$ is supposed to be less than $n$, $\lfloor\underline{r}$ is prime to $n$.

Hence, $\lfloor\underline{r}$ is a divisor of $(n-1)(n-2) \ldots (n-r+1)$

and $n(n-1) \ldots (n-r+1)/\lfloor\underline{r}$ is divisible by $n$.

Thus *if n is a prime, all the coefficients in the expansion of $(1 + x)^n$, except the first and last, are divisible by n.*

**Note:** The reader is supposed to be acquainted with what is said in elementary textbooks about 'permutations and combinations' and the 'binomial theorem for a positive integral index.' In what follows, $P_r^n$, denotes the number of permutations, and $C_r^n$ the number of combinations, of *n things taken r at a time.*

**Example 1.** *Find the highest power of 5 contained in $\lfloor\underline{158}$ .*

We have $I[158/5] = 31$, $I[158/5^2] = I[31/5] = 6$, $I[158/5^3] = I[6/5] = 1$: therefore the required power has an index $= 31 + 6 + 1 = 38$.

**Example 2.** *If n is an odd prime, the integral part of* $(\sqrt{5}+2)^n - 2^{n+1}$ *is divisible by 20n.*

Let $(\sqrt{5}+2)^n = N + f$ where $0 < f < 1$; and let $(\sqrt{5}+2)^n = f'$. Then, since $0 < \sqrt{5} - 2 < 1$, we have also $0 < f' < 1$.

Again, since $n$ is odd, $N + f - f' = (\sqrt{5}+2)^n - (\sqrt{5}-2)^n$ = an integer; hence, since $f$ and $f'$ are positive and less than 1, $f = f'$, and thus

$$N = 2\,(C_1^n \,.\, 2 \,.\, 5^{\frac{1}{2}(n-1)} + C_3^n \,.\, 2^3 \,.\, 5^{\frac{1}{2}(n-3)} + \ldots + C_2^n \,.\, 2^{n-2} \,.\, 5 + 2^n).$$

Moreover, since $n$ is a prime, $C_r^n$, is divisible by $n$, and therefore $N - 2^{n+1}$ is divisible by $20n$; which is the required result.

**10. Numbers in Arithmetical Progression:**

**(1)** *Let a be prime to n, then if the first n terms of the arithmetical progression x, x + a, x + 2a, ... , are divided by n, the remainders are the numbers 0, 1, 2, ..., n – 1*, taken in a certain order.

If we suppose that two of the terms as $x + ma$, $x + m'a$ leave equal remainders, then their difference $(m - m')\,a$ would be divisible by $n$. This is impossible, for $a$ is prime to $n$ and $|\,m - m'\,| < n$.

Therefore the remainders are all different, and as each is less than $n$, they must be numbers 0, 1, 2, ..., $n - 1$, taken in some order or other.

*If the progression is continued beyond the n-th term, the remainders recur in the same order.*

For the terms $x + ma$, $x + m'a$ leave the same remainder if $m = m' + qn$.

**(2)** *If a and n are not prime to one another and g is their greatest common divisor, the remainder recur in a cycle of n/g numbers*.

For let $a = ga'$, $n = gn'$, so that $a'$ is prime to $n'$. The terms $x + ma$, $x + m'a$ leave the same remainder if, and only if, $a\,(m - m')$ is divisible by $n$, that is, if $a'\,(m - m')$ is divisible by $n'$. Since $a'$ is prime to $n'$, this can only happen when $m - m'$ is divisible by $n'$. Thus the first $n'$ terms leave different remainders and, after that, they recur in order.

**11. Method of Induction:** Many theorems relating to whole numbers can be proved by a process known as *mathematical induction*. In some cases this is the only method available. The method may be described as follows.

Let $f\,(n)$ be a function of an integral variable $n$. Suppose that a certain statement $S$, relating to $f\,(n)$, is true when $n = a$.

Further, suppose we can prove that, if $S$ is true when $n = m$, it is also true when $n = m + 1$.

Then since $S$ is true when $n = a$, it is true when $n = a + 1$, $a + 2$, $a + 3$, ... in succession, that is, when $n \geq a$.

**Example 1.** *Show that* $2^{2n} - 3n - 1$ *is divisible by 9*.

Let $f\,(n) = 2^{2n} - 3n - 1$, then $f\,(1) = 0$ and 0 is divisible by 9, so the theorem is true for $n = 1$.

Again, $f\,(n + 1) - f\,(n) = 2^{2(n+1)} - 2^{2n} - 3 = 3\,(2^{2n} - 1)$.

Also $2^{2n} - 1 = (3 + 1)^n - 1 = 3k$, where $k$ in an integer,

$\therefore \quad f(n + 1) - f(n) = 9k.$

Hence if $f(n)$ is divisible by 9, so is $f(n + 1)$; and, since $f(1)$ is so divisible, it follows in succession that $f(2), f(3), f(4)$, etc., are so divisible; that is, the theorem holds for all values of $n$.

Or more easily, using the method of (9) Ex. 2, $f(n) = (3 + 1)^n - 3n - 1$, etc.

**EXAMPLE 2.** *If n is a positive integer, prove that*

$$\frac{1}{n}+\frac{1}{n+1}+\frac{1}{n+2}+\ldots+\frac{1}{2n-1} = 1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\ldots+\frac{1}{2n-1}.$$

If $$u_n = \frac{1}{n}+\frac{1}{n+1}+\ldots+\frac{1}{2n-1},$$

then $$u_{n+1} = \frac{1}{n+1}+\ldots+\frac{1}{2n-1}+\frac{1}{2n}+\frac{1}{2n+1};$$

$\therefore$ $$u_{n+1} - u_n = \frac{1}{2n}+\frac{1}{2n+1}-\frac{1}{n} = -\frac{1}{2n}+\frac{1}{2n+1}.$$

Again, if $$v_n = 1-\frac{1}{2}+\frac{1}{3}-\ldots+\frac{1}{2n-1},$$

then $$v_{n+1} = 1-\frac{1}{2}+\frac{1}{3}-\ldots+\frac{1}{2n-1}-\frac{1}{2n}+\frac{1}{2n+1};$$

$\therefore$ $$v_{n+1} - v_n = -\frac{1}{2n}+\frac{1}{2n+1} = u_{n+1} - u_n.$$

Hence if $u_n = v_n$, then $u_{n+1} = v_{n+1}$. Now the statement holds for $n = 1$; hence, in succession, it is true for $n = 2, 3, 4, \ldots$, that is, for any value of $n$.

## EXERCISE I

1. If $q$ is the quotient and $r$ the remainder when $a$ is divided by $b$, show that $q$ is the quotient when $a$ is divided by $b + 1$, provided that $r \geq q$.
2. If $a$ and $b$ are prime to each other, show that
   (*i*) $a + b$ and $a - b$ have no common factor other than 2;
   (*ii*) $a^2 - ab + b^2$ and $a + b$ have no common factor other than 3.
3. If $a$ and $b$ are prime to each other, and $n$ is a prime, prove that
   $$(a^n + b^n) / (a + b) \text{ and } a + b$$
   have no common factor, unless $a + b$ is a multiple of $n$.
4. If $a$ is prime to $b$ and $y$, and $b$ is prime to $x$, then $ax + by$ is prime to $ab$.
5. If $X = ax + by$ and $Y = a'x + b'y$, where $ab' - a'b = 1$, the greatest common divisor of $X$ and $Y$ is the same as that of $x$ and $y$.
6. If $p$ is a prime, and $p = a^2 - b^2$, then $a = \frac{1}{2}(p + 1)$, $b = \frac{1}{2}(p - 1)$.

**7.** Express 55 in the form $a^2 - b^2$ in two ways.

**8.** If $x$ takes the values 1, 2, 3, ... , in the expressions

($i$) $x^2 + x + 17$, ($ii$) $2x^2 + 29$,

($iii$) $x^2 + x + 41$,

the resulting values of the expressions are primes, provided that in ($i$) $x < 16$, in ($ii$) $x < 29$, and in ($iii$) $x < 40$.

Verify for $x = 15, 28, 39$ repectively.

**9.** If $f(x)$ is a polynomial, it cannot represent primes only.

[Let $u = f(x)$ and $v = f(x + ku)$, where $k$ is any integer. Prove that $u$ is a factor of $v$.]

**10.** For the values 2, 3, 4, ... 10 of $x$, the number $2.3.5.7 + x$ is composite. Hence write down nine consecutive numbers none of which is a prime.

**11.** If $n$ is any odd number, then $n(n^2 - 1)$ is divisible by 24; and if $n$ is an odd prime greater than 3, then $n^2 - 1$ is divisible by 24.

**12.** Show that $2^n + 1$ or $2^n - 1$ is divisible by 3, according as $n$ is odd or even.

**13.** If $n$ is prime to 5, then $n^2 + 1$ or $n^2 - 1$ is divisible by 5, and therefore $n^4$ is of the form $5m + 1$.

**14.** If $n$ is prime to 5, then $n^5 - n$ is divisible by 30; hence the fifth power of any number has the same right-hand digit as the number itself.

**15.** Show that $2^{2n} + 1$ or $2^{2n} - 1$ is divisible by 5, according as $n$ is odd or even.

**16.** Show that $5^{2n} + 1$ or $5^{2n} - 1$ is divisible by 13, according as $n$ is odd or even.

**17.** If $3^n - 1$ is divided by 13, show that the remainder is either 0, 2, or 8, according as $n$ is of the form $3m$, $3m + 1$, or $3m - 1$; hence prove that $3^n - 1$ or $3^{2n} + 3^n + 1$ is divisible by 13, according as $n$ is, or is not, a multiple of 3.

**18.** If $2^n + 1$ is a prime, then $n$ must be a power of 2.

**19.** Show that $7^{2n} - 48n - 1$ is divisible by 2304.

**20.** Show that $7^{2n} + 16n - 1$ is divisible by 64.

**21.** Prove that $2^{2n+1} - 9n^2 + 3n - 2$ is divisible by 54.

**22.** Find the number of divisors of 2000, and their sum.

**23.** Let $s$ be the sum of the divisors of $N$, excluding $N$ itself; if $s = N$, then $n$ is called a *perfect number.*

Show that, if $2^n - 1$ is a prime, then $2^{n-1}(2^n - 1)$ is a perfect number; and find the three least numbers given by this formula.

**24.** If $n, r, s$ are the numbers, and $P, R, S$ the products, of the divisors of $N$, $L$, $M$ respectively, where $N = LM$, and $L$ and $M$ are prime to one another, prove that ($i$) $n = r \cdot s$, ($ii$) $P = R^s \cdot S^r$.

**25.** If $n$ is the number, and $P$ the product, of the divisors of $N$, prove that $P^2 = N^n$.

**26.** If the product of the divisors of $N$, excluding $N$ itself, is equal to $N$, then $N$ is the product of two primes or the cube of a prime.

**27.** If $N$ has 16 divisors, it cannot have more than 4 prime factors, $a, b, c, d$, and it must be of one of the forms $abcd$, $a^3b^3$, $a^3bc$, $a^7b$, $a^{15}$. Hence find the smallest number having 16 divisors.

**28.** Find the smallest number with 24 divisors.

**29.** Prove by induction that $n(n + 1)(n + 2)... (n + r - 1)$ is divisible by $\underline{|r}$.

**30.** Find the highest power of the prime $p$ in $\underline{|N}$, when

($i$) $p^r - 1 < N < p^r + p$; ($ii$) $p^r - p < N < p^r$.

**31.** If $N$ is expressed as a polynomial in a prime $p$, with each of the coefficients less than $p$, and $s$ is the sum of these coefficients, prove that the power of $p$ contained in $\lfloor\underline{N}$ is $(N - s)/(p - 1)$.

**32.** Show that the index of the highest power of 2 contained in $\lfloor\underline{N}$ is $N - 1$ when $N$ is a power of 2, and $N - r$ when $N$ is equal to $2^r - 1$.

**33.** Show that $\lfloor\underline{2n-1}\big/\big(\lfloor\underline{n}\lfloor\underline{n-1}\big)$ is odd or even according as $n$ is, or is not, a power of 2.

**34.** Prove that $\lfloor\underline{2n}$ is divisible by $\lfloor\underline{n}.\lfloor\underline{n+1}$.

**35.** Prove that, if $g$ is the greatest common divisor of $m$ and $n + 1$, then $g.\ \lfloor\underline{m+n}$ is divisible by $\lfloor\underline{m}.\lfloor\underline{n+1}$.

**36.** Prove that the power of 2 in $\lfloor\underline{3n}$ is greater than or equal to the power of 2 in $\lfloor\underline{n}.\lfloor\underline{n+1}.\lfloor\underline{n+2}$ .

**37.** Prove that, if $n$ is greater than 2, then $\lfloor\underline{3n}$ is divisible by $\lfloor\underline{n}.\lfloor\underline{n+1}.\lfloor\underline{n+2}$.

**38.** If $a$, $b$, $c$, ..., are numbers whose sum is a prime, $p$, then

$\lfloor\underline{p}\big/\big(\lfloor\underline{a}.\lfloor\underline{b}.\lfloor\underline{c}...\big)$ is an integer divisible by $p$.

**39.** If $u_n = (3 + \sqrt{5})^n + (3 - \sqrt{5})^n$, show that $u_n$ is an integer, and that

$$u_{n+1} = 6u_n - 4u_{n-1}.$$

Hence prove that the integer next greater than $\left(3+\sqrt{5}\right)^n$ is divisible by $2^n$.

**40.** The integer next greater than $\left(\sqrt{7} + \sqrt{3}\right)^{2n}$ is divisible by $2^{2n}$.

**41.** If $2^n + 1 = xy$, prove that $x - 1$ and $y - 1$ are divisible by the same power of 2.

■■■