CHAPTER XXX.

Theory of Numbers.

407. In this chapter we shall use the word *number* as equivalent in meaning to *positive integer*.

A number which is not exactly divisible by any number except itself and unity is called a *prime number*, or a *prime;* a number which is divisible by other numbers besides itself and unity is called a *composite number*; thus 53 is a prime number, and 35 is a composite number. Two numbers which have no common factor except unity are said to be prime to each other; thus 24 is prime to 77.

408. We shall make frequent use of the following elementary propositions, some of which arise so naturally out of the definition of a prime that they may be regarded as axioms.

(i) If a number a divides a product bc and is prime to one factor b, it must divide the other factor c.

For since a divides bc, every factor of a is found in bc; but since a is prime to b, no factor of a is found in b; therefore all the factors of a are found in c; that is, a divides c.

(ii) If a prime number a divides a product $bcd\ldots$, it must divide one of the factors of that product; and therefore if a prime number a divides b^n, where n is any positive integer, it must divide b.

(iii) If a is prime to each of the numbers b and c, it is prime to the product bc. For no factor of a can divide b or c; therefore the product bc is not divisible by any factor of a, that is, a is prime to bc. Conversely if a is prime to bc, it is prime to each of the numbers b and c.

Also if a is prime to each of the numbers b, c, d, ..., it is prime to the product $bcd\ldots$; and conversely if a is prime to any number, it is prime to every factor of that number.

(iv) If a and b are prime to each other, every positive integral power of a is prime to every positive integral power of b. This follows at once from (iii).

(v) If a is prime to b, the fractions $\frac{a}{b}$ and $\frac{a^n}{b^m}$ are in their lowest terms, n and m being any positive integers. Also if $\frac{a}{b}$ and $\frac{c}{d}$ are any two equal fractions, and $\frac{a}{b}$ is in its lowest terms, then c and d must be equimultiples of a and b respectively.

409. *The number of primes is infinite.*

For if not, let p be the greatest prime number; then the product $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \ldots p$, in which each factor is a prime number, is divisible by each of the factors 2, 3, 5, $\ldots p$; and therefore the number formed by adding unity to their product is not divisible by any of these factors; hence it is either a prime number itself or is divisible by some prime number greater than p: in either case p is not the *greatest* prime number, and therefore the number of primes is not limited.

410. *No rational algebraical formula can represent prime numbers only.*

If possible, let the formula $a + bx + cx^2 + dx^3 + \ldots$ represent prime numbers only, and suppose that when $x = m$ the value of the expression is p, so that

$$p = a + bm + cm^2 + dm^3 + \ldots\ldots;$$

when $x = m + np$ the expression becomes

$$a + b(m + np) + c(m + np)^2 + d(m + np)^3 + \ldots,$$

that is, $a + bm + cm^2 + dm^3 + \ldots +$ a multiple of p,

or $p +$ a multiple of p,

thus the expression is divisible by p, and is therefore not a prime number.

411. *A number can be resolved into prime factors in only one way.*

Let N denote the number; suppose $N = abcd\ldots$, where a, b, c, d, ... are prime numbers. Suppose also that $N = \alpha\beta\gamma\delta\ldots$, where α, β, γ, δ, ... are other prime numbers. Then

$$abcd\ldots = \alpha\beta\gamma\delta\ldots;$$

hence α must divide $abcd\ldots$; but each of the factors of this product is a prime, therefore α must divide one of them, a suppose. But α and a are both prime; therefore α must be equal to a. Hence $bcd\ldots = \beta\gamma\delta\ldots$; and as before, β must be equal to one of the factors of $bcd\ldots$; and so on. Hence the factors in $\alpha\beta\gamma\delta\ldots$ are equal to those in $abcd\ldots$, and therefore N can only be resolved into prime factors in one way.

412. *To find the number of divisors of a composite number.*

Let N denote the number, and suppose $N = a^p b^q c^r \ldots$, where a, b, c, ... are different prime numbers and p, q, r, ... are positive integers. Then it is clear that each term of the product

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

is a divisor of the given number, and that no other number is a divisor; hence the number of divisors is the number of terms in the product, that is,

$$(p + 1)(q + 1)(r + 1)\ldots\ldots$$

This includes as divisors, both unity and the number itself.

413. *To find the number of ways in which a composite number can be resolved into two factors.*

Let N denote the number, and suppose $N = a^p b^q c^r \ldots$, where a, b, $c\ldots$ are different prime numbers and p, q, $r\ldots$ are positive integers. Then each term of the product

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

is a divisor of N; but there are *two* divisors corresponding to each way in which N can be resolved into two factors; hence the required number is

$$\frac{1}{2}(p + 1)(q + 1)(r + 1)\ldots\ldots$$

This supposes N not a perfect square, so that one at least of the quantities p, q, r, ... is an odd number.

If N is a perfect square, one way of resolution into factors is $\sqrt{N} \times \sqrt{N}$, and to this way there corresponds only *one* divisor $\sqrt{N}$. If we exclude this, the number of ways of resolution is

$$\frac{1}{2}\left\{(p + 1)(q + 1)(r + 1)\ldots - 1\right\},$$

and to this we must add the one way $\sqrt{N} \times \sqrt{N}$; thus we obtain for the required number

$$\frac{1}{2}\left\{(p + 1)(q + 1)(r + 1)\ldots + 1\right\}.$$

414. *To find the number of ways in which a composite number can be resolved into two factors which are prime to each other.*

As before, let the number $N = a^p b^q c^r \ldots$. Of the two factors one must contain a^p, for otherwise there would be some power of a in one factor and some power of a in the other factor, and thus the two factors would not be prime to each other. Similarly b^q must occur in one of the factors only; and so on. Hence the required number is equal to the number of ways in which the product $abc\ldots$ can be resolved into two factors; that is, the number of ways is $\frac{1}{2}(1+1)(1+1)(1+1)\ldots$ or 2^{n-1}, where n is the number of *different* prime factors in N.

415. *To find the sum of the divisors of a number.*

Let the number be denoted by $a^p b^q c^r \ldots$, as before. Then each term of the product

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

is a divisor, and therefore the *sum* of the divisors is equal to this product; that is,

$$\text{the sum required} = \frac{a^{p+1}-1}{a-1} \cdot \frac{b^{q+1}-1}{b-1} \cdot \frac{c^{r+1}-1}{c-1} \ldots .$$

Example 1. Consider the number 21600.

Since $21600 = 6^3 \cdot 10^2 = 2^3 \cdot 3^3 \cdot 2^2 \cdot 5^2 = 2^5 \cdot 3^3 \cdot 5^2$,

$$\text{the number of divisors} = (5+1)(3+1)(2+1) = 72;$$

$$\text{the sum of the divisors} = \frac{2^6-1}{2-1} \cdot \frac{3^4-1}{3-1} \cdot \frac{5^3-1}{5-1}$$
$$= 63 \times 40 \times 31$$
$$= 78120.$$

Also 21600 can be resolved into two factors prime to each other in 2^{3-1}, or 4 ways.

Example 2. If n is odd shew that $n(n^2-1)$ is divisible by 24.

We have $n(n^2-1) = n(n-1)(n+1)$.

Since n is odd, $n-1$ and $n+1$ are two consecutive even numbers; hence one of them is divisible by 2 and the other by 4.

Again $n-1$, n, $n+1$ are three consecutive numbers; hence one of them is divisible by 3. Thus the given expression is divisible by the product of 2, 3, and 4, that is, by 24.

Example 3. Find the highest power of 3 which is contained in $\lfloor 100$.

Of the first 100 integers, as many are divisible by 3 as the number of times that 3 is contained in 100, that is, 33; and the integers are 3, 6, 9,...99. Of these, some contain the factor 3 again, namely 9, 18, 27,...99, and their number is the quotient of 100 divided by 9. Some again of these last integers contain the factor 3 a third time, namely 27, 54, 81, the number of them being the quotient of 100 by 27. One number only, 81, contains the factor 3 four times.

Hence the highest power required $= 33 + 11 + 3 + 1 = 48$.

This example is a particular case of the theorem investigated in the next article.

416. *To find the highest power of a prime number* a *which is contained in* $\lfloor n$.

Let the greatest integer contained in $\frac{n}{a}$, $\frac{n}{a^2}$, $\frac{n}{a^3}$, ... respectively be denoted by $I\left(\frac{n}{a}\right)$, $I\left(\frac{n}{a^2}\right)$, $I\left(\frac{n}{a^3}\right)$, ... Then among the numbers 1, 2, 3, ... n, there are $I\left(\frac{n}{a}\right)$ which contain a at least once, namely the numbers a, $2a$, $3a$, $4a$, ... Similarly there are $I\left(\frac{n}{a^2}\right)$ which contain a^2 at least once, and $I\left(\frac{n}{a^3}\right)$ which contain a^3 at least once; and so on. Hence the highest power of a contained in $\lfloor n$ is

$$I\left(\frac{n}{a}\right) + I\left(\frac{n}{a^2}\right) + I\left(\frac{n}{a^3}\right) + \ldots$$

417. In the remainder of this chapter we shall find it convenient to express a multiple of n by the symbol $M(n)$.

418. *To prove that the product of* r *consecutive integers is divisible by* $\lfloor r$.

Let P_n stand for the product of r consecutive integers, the least of which is n; then

$$P_n = n(n+1)(n+2)\ldots(n+r-1),$$

and
$$P_{n+1} = (n+1)(n+2)(n+3)\ldots(n+r);$$

$$\therefore\ nP_{n+1} = (n+r)P_n = nP_n + rP_n;$$

$$\therefore\ P_{n+1} - P_n = \frac{P_n}{n} \times r$$

$= r$ times the product of $r-1$ consecutive integers.

Hence if the product of $r-1$ consecutive integers is divisible by $\lfloor\underline{r-1}$, we have

$$P_{n+1} - P_n = rM(\lfloor\underline{r-1})$$
$$= M(\lfloor\underline{r}).$$

Now $P_1 = \lfloor\underline{r}$, and therefore P_2 is a multiple of $\lfloor\underline{r}$; therefore also P_3, P_4, ... are multiples of $\lfloor\underline{r}$. We have thus proved that if the product of $r-1$ consecutive integers is divisible by $\lfloor\underline{r-1}$, the product of r consecutive integers is divisible by $\lfloor\underline{r}$; but the product of every two consecutive integers is divisible by $\lfloor\underline{2}$; therefore the product of every three consecutive integers is divisible by $\lfloor\underline{3}$; and so on generally.

This proposition may also be proved thus:

By means of Art. 416, we can shew that every prime factor is contained in $\lfloor\underline{n+r}$ as often *at least* as it is contained in $\lfloor\underline{n} \lfloor\underline{r}$.

This we leave as an exercise to the student.

419. *If* p *is a prime number, the coefficient of every term in the expansion of* $(a+b)^p$, *except the first and last, is divisible by* p.

With the exception of the first and last, every term has a coefficient of the form

$$\frac{p(p-1)(p-2)\ldots(p-r+1)}{\lfloor\underline{r}},$$

where r may have any integral value not exceeding $p-1$. Now this expression is an integer; also since p is prime no factor of $\lfloor\underline{r}$ is a divisor of it, and since p is greater than r it cannot divide any factor of $\lfloor\underline{r}$; that is, $(p-1)(p-2)\ldots(p-r+1)$ must be divisible by $\lfloor\underline{r}$. Hence every coefficient except the first and the last is divisible by p.

420. *If* p *is a prime number, to prove that*

$$(a+b+c+d+\ldots)^p = a^p + b^p + c^p + d^p + \ldots + M(p).$$

Write β for $b+c+\ldots$; then by the preceding article

$$(a+\beta)^p = a^p + \beta^p + M(p).$$

Again $\beta^p = (b+c+d+\ldots)^p = (b+\gamma)^p$ suppose;

$$= b^p + \gamma^p + M(p).$$

By proceeding in this way we may establish the required result.

421. [Fermat's Theorem.] *If* p *is a prime number and* N *is prime to* p, *then* $N^{p-1}-1$ *is a multiple of* p.

We have proved that

$$(a+b+c+d+\ldots)^p = a^p + b^p + c^p + d^p + \ldots + M(p);$$

let each of the quantities a, b, c, d, ... be equal to unity, and suppose they are N in number; then

$$N^p = N + M(p);$$

that is,
$$N(N^{p-1}-1) = M(p).$$

But N is prime to p, and therefore $N^{p-1}-1$ is a multiple of p.

Cor. Since p is prime, $p-1$ is an even number except when $p=2$. Therefore

$$(N^{\frac{p-1}{2}}+1)(N^{\frac{p-1}{2}}-1) = M(p).$$

Hence either $N^{\frac{p-1}{2}}+1$ or $N^{\frac{p-1}{2}}-1$ is a multiple of p,

that is $N^{\frac{p-1}{2}} = Kp \pm 1$, where K is some positive integer.

422. It should be noticed that in the course of Art. 421 it was shewn that $N^p - N = M(p)$ *whether* N *is prime to* p *or not*; this result is sometimes more useful than Fermat's theorem.

Example 1. Shew that $n^7 - n$ is divisible by 42.

Since 7 is a prime,
$$n^7 - n = M(7);$$

also
$$n^7 - n = n(n^6-1) = n(n+1)(n-1)(n^4+n^2+1).$$

Now $(n-1)\,n\,(n+1)$ is divisible by $\underline{|3}$; hence n^7-n is divisible by 6×7, or 42.

Example 2. If p is a prime number, shew that the difference of the p^{th} powers of any two numbers exceeds the difference of the numbers by a multiple of p.

Let x, y be the numbers; then

$$x^p - x = M(p) \text{ and } y^p - y = M(p),$$

that is,
$$x^p - y^p - (x-y) = M(p);$$

whence we obtain the required result.

Example 3. Prove that every square number is of the form $5n$ or $5n \pm 1$.

If N is not prime to 5, we have $N^2 = 5n$ where n is some positive integer. If N is prime to 5 then N^4-1 is a multiple of 5 by Fermat's theorem; thus either N^2-1 or N^2+1 is a multiple of 5; that is, $N^2 = 5n \pm 1$.

EXAMPLES. XXX. a.

1. Find the least multipliers of the numbers

3675, 4374, 18375, 74088

respectively, which will make the products perfect squares.

2. Find the least multipliers of the numbers

7623, 109350, 539539

respectively, which will make the products perfect cubes.

3. If x and y are positive integers, and if $x-y$ is even, shew that x^2-y^2 is divisible by 4.

4. Shew that the difference between any number and its square is even.

5. If $4x-y$ is a multiple of 3, shew that $4x^2+7xy-2y^2$ is divisible by 9.

6. Find the number of divisors of 8064.

7. In how many ways can the number 7056 be resolved into two factors?

8. Prove that $2^{4n}-1$ is divisible by 15.

9. Prove that $n(n+1)(n+5)$ is a multiple of 6.

10. Shew that every number and its cube when divided by 6 leave the same remainder.

11. If n is even, shew that $n(n^2+20)$ is divisible by 48.

12. Shew that $n(n^2-1)(3n+2)$ is divisible by 24.

13. If n is greater than 2, shew that n^5-5n^3+4n is divisible by 120.

14. Prove that $3^{2n}+7$ is a multiple of 8.

15. If n is a prime number greater than 3, shew that n^2-1 is a multiple of 24.

16. Shew that n^5-n is divisible by 30 for all values of n, and by 240 if n is odd.

17. Shew that the difference of the squares of any two prime numbers greater than 6 is divisible by 24.

18. Shew that no square number is of the form $3n-1$.

19. Shew that every cube number is of the form $9n$ or $9n\pm1$.

20. Shew that if a cube number is divided by 7, the remainder is 0, 1 or 6.

21. If a number is both square and cube, shew that it is of the form $7n$ or $7n+1$.

22. Shew that no triangular number can be of the form $3n-1$.

23. If $2n+1$ is a prime number, shew that 1^2, 2^2, 3^2,...n^2 when divided by $2n+1$ leave different remainders.

24. Shew that a^x+a and a^x-a are always even, whatever a and x may be.

25. Prove that every even power of every odd number is of the form $8r+1$.

26. Prove that the 12^{th} power of any number is of the form $13n$ or $13n+1$.

27. Prove that the 8^{th} power of any number is of the form $17n$ or $17n\pm1$.

28. If n is a prime number greater than 5, shew that n^4-1 is divisible by 240

29. If n is any prime number greater than 3, except 7, shew that n^6-1 is divisible by 168.

30. Show that $n^{36}-1$ is divisible by 33744 if n is prime to 2, 3, 19 and 37.

31. When $p+1$ and $2p+1$ are both prime numbers, shew that $x^{2p}-1$ is divisible by $8(p+1)(2p+1)$, if x is prime to 2, $p+1$, and $2p+1$.

32. If p is a prime, and x prime to p, shew that $x^{p^r-p^{r-1}}-1$ is divisible by p^r.

33. If m is a prime number, and a, b two numbers less than m, prove that

$$a^{m-2}+a^{m-3}b+a^{m-4}b^2+\ldots\ldots+b^{m-2}$$

is a multiple of m.

423. If a is any number, then any other number N may be expressed in the form $N=aq+r$, where q is the integral quotient when N is divided by a, and r is a remainder less than a. The number a, to which the other is referred, is sometimes called the *modulus;* and to any given modulus a there are a different

forms of a number N, each form corresponding to a different value of r. Thus to modulus 3, we have numbers of the form $3q$, $3q+1$, $3q+2$; or, more simply, $3q$, $3q \pm 1$, since $3q+2$ is equal to $3(q+1)-1$. In like manner to modulus 5 any number will be one of the five forms $5q$, $5q \pm 1$, $5q \pm 2$.

424. If b, c are two integers, which when divided by a leave the same remainder, they are said to be **congruent** with respect to the modulus a. In this case $b-c$ is a multiple of a, and following the notation of Gauss we shall sometimes express this as follows:

$$b \equiv c \text{ (mod. } a), \text{ or } b - c \equiv 0 \text{ (mod. } a).$$

Either of these formulæ is called a **congruence.**

425. *If* b, c *are congruent with respect to modulus* a, *then* pb *and* pc *are congruent,* p *being any integer.*

For, by supposition, $b - c = na$, where n is some integer; therefore $pb - pc = pna$; which proves the proposition.

426. *If* a *is prime to* b, *and the quantities*

$$\text{a, } 2\text{a, } 3\text{a, } \ldots\ldots \text{ (b} - 1)\text{ a}$$

are divided by b, *the remainders are all different.*

For if possible, suppose that two of the quantities ma and $m'a$ when divided by b leave the same remainder r, so that

$$ma = qb + r, \quad m'a = q'b + r;$$

then

$$(m - m')\, a = (q - q')\, b;$$

therefore b divides $(m-m')\,a$; hence it must divide $m-m'$, since it is prime to a; but this is impossible since m and m' are each less than b.

Thus the remainders are all different, and since none of the quantities is exactly divisible by b, the remainders must be the terms of the series 1, 2, 3, ... $b-1$, but not necessarily in this order.

Cor. If a is prime to b, and c is any number, the b terms of the A. P.

$$c,\ c+a,\ c+2a,\ \ldots\ldots\ c+(b-1)\,a,$$

when divided by b will leave the same remainders as the terms of the series

$$c,\ c+1,\ c+2,\ \ldots\ldots\ c+(b-1),$$

though not necessarily in this order; and therefore the remainders will be $0,\ 1,\ 2,\ \ldots\ldots\ b-1$.

427. *If* $b_1, b_2, b_3, \ldots$ *are respectively congruent to* $c_1, c_2, c_3, \ldots$ *with regard to modulus* a, *then the products* $b_1b_2b_3\ldots,\ c_1c_2c_3\ldots$ *are also congruent.*

For by supposition,

$$b_1 - c_1 = n_1 a,\quad b_2 - c_2 = n_2 a,\quad b_3 - c_3 = n_3 a,\ \ldots$$

where $n_1,\ n_2,\ n_3\ \ldots$ are integers;

$$\begin{aligned}\therefore\ b_1b_2b_3\ldots &= (c_1 + n_1 a)\,(c_2 + n_2 a)\,(c_3 + n_3 a)\ldots \\ &= c_1c_2c_3\ \ldots\ + M(a),\end{aligned}$$

which proves the proposition.

428. We can now give another proof of Fermat's Theorem.

If p *be a prime number and* N *prime to* p, *then* $N^{p-1} - 1$ *is a multiple of* p.

Since N and p are prime to each other, the numbers

$$N,\ 2N,\ 3N,\ \ldots\ldots\ (p-1)\,N\ldots\ldots\ldots\ldots\ldots(1),$$

when divided by p leave the remainders

$$1,\ 2,\ 3,\ \ldots\ldots\ (p-1)\ \ldots\ldots\ldots\ldots\ldots\ldots(2),$$

though not necessarily in this order. Therefore the product of all the terms in (1) is congruent to the product of all the terms in (2), p being the modulus.

That is, $\underline{|p-1}\ N^{p-1}$ and $\underline{|p-1}$ leave the same remainder when divided by p; hence

$$\underline{|p-1}\,(N^{p-1} - 1) = M(p);$$

but $\underline{|p-1}$ is prime to p; therefore it follows that

$$N^{p-1} - 1 = M(p).$$

429. We shall denote the number of integers less than a number a and prime to it by the symbol $\phi(a)$; thus $\phi(2) = 1$; $\phi(13) = 12$; $\phi(18) = 6$; the integers less than 18 and prime to it being 1, 5, 7, 11, 13, 17. It will be seen that we here consider unity as prime to all numbers.

430. *To shew that if the numbers* a, b, c, d, ... *are prime to each other,*

$$\phi(\text{abcd}\ldots) = \phi(\text{a}) \cdot \phi(\text{b}) \cdot \phi(\text{c}) \ldots .$$

Consider the product ab; then the first ab numbers can be written in b lines, each line containing a numbers; thus

$$\begin{array}{llll} 1, & 2, \ldots\ldots & k, \ldots\ldots & a, \\ a+1, & a+2, \ldots\ldots & a+k, \ldots\ldots & a+a, \\ 2a+1, & 2a+2, \ldots\ldots & 2a+k, \ldots\ldots & 2a+a, \\ \ldots & \ldots\ldots\ldots\ldots\ldots\ldots & & \\ (b-1)a+1, & (b-1)a+2, \ldots & (b-1)a+k, \ldots & (b-1)a+a. \end{array}$$

Let us consider the vertical column which begins with k; if k is prime to a all the terms of this column will be prime to a; but if k and a have a common divisor, no number in the column will be prime to a. Now the first row contains $\phi(a)$ numbers prime to a; therefore there are $\phi(a)$ vertical columns in each of which every term is prime to a; let us suppose that the vertical column which begins with k is one of these. This column is an A.P., the terms of which when divided by b leave remainders 0, 1, 2, 3, ... $b-1$ [Art. 426 Cor.]; hence the column contains $\phi(b)$ integers prime to b.

Similarly, each of the $\phi(a)$ vertical columns in which every term is prime to a contain $\phi(b)$ integers prime to b; hence in the table there are $\phi(a) \cdot \phi(b)$ integers which are prime to a and also to b, and therefore to ab; that is

$$\phi(ab) = \phi(a) \cdot \phi(b).$$

Therefore
$$\begin{aligned} \phi(abcd\ldots) &= \phi(a) \cdot \phi(bcd\ldots) \\ &= \phi(a) \cdot \phi(b) \cdot \phi(cd\ldots) \\ &= \phi(a) \cdot \phi(b) \cdot \phi(c) \cdot \phi(d) \ldots . \end{aligned}$$

431. *To find the number of positive integers less than a given number, and prime to it.*

Let N denote the number, and suppose that $N = a^p b^q c^r \ldots$, where a, b, c, ... are different prime numbers, and p, q, r ... positive integers. Consider the factor a^p; of the natural numbers 1, 2, 3, ... $a^p - 1$, a^p, the only ones not prime to a are

$$a,\ 2a,\ 3a,\ \ldots\ (a^{p-1}-1)a,\ (a^{p-1})a,$$

and the number of these is a^{p-1}; hence

$$\phi(a^p) = a^p - a^{p-1} = a^p\left(1 - \frac{1}{a}\right).$$

Now all the factors a^p, b^q, c^r, ... are prime to each other;

$$\therefore\ \phi(a^p b^q c^r \ldots) = \phi(a^p) \cdot \phi(b^q) \cdot \phi(c^r) \ldots$$

$$= a^p\left(1 - \frac{1}{a}\right) \cdot b^q\left(1 - \frac{1}{b}\right) \cdot c^r\left(1 - \frac{1}{c}\right) \ldots$$

$$= a^p b^q c^r \ldots \left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right) \ldots;$$

that is,
$$\phi(N) = N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right) \ldots.$$

Example. Shew that the sum of all the integers which are less than N and prime to it is $\frac{1}{2}N\phi(N)$.

If x is any integer less than N and prime to it, then $N - x$ is also an integer less than N and prime to it.

Denote the integers by 1, p, q, r, ..., and their sum by S; then

$$S = 1 + p + q + r + \ldots + (N-r) + (N-q) + (N-p) + (N-1),$$

the series consisting of $\phi(N)$ terms.

Writing the series in the reverse order,

$$S = (N-1) + (N-p) + (N-q) + (N-r) + \ldots + r + q + p + 1;$$

$\therefore$ by addition, $2S = N + N + N + \ldots$ to $\phi(N)$ terms;

$$\therefore\ S = \tfrac{1}{2}N\phi(N).$$

432. From the last article it follows that the number of integers which are less than N and *not* prime to it is

$$N - N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right)\left(1 - \frac{1}{d}\right) \ldots;$$

that is,

$$\frac{N}{a} + \frac{N}{b} + \frac{N}{c} + \ldots - \frac{N}{ab} - \frac{N}{ac} - \frac{N}{bc} - \ldots + \frac{N}{abc} + \ldots.$$

Here the term $\frac{N}{a}$ gives the number of the integers

$$a,\ 2a,\ 3a,\ \ldots\ \frac{N}{a} \cdot a$$

which contain a as a factor; the term $\frac{N}{ab}$ gives the number of

the integers ab, $2ab$, $3ab$, ... $\frac{N}{ab}\,ab$, which contain ab as a factor, and so on. Further, every integer is reckoned once, and once only; thus, each multiple of ab will appear once among the multiples of a, once among the multiples of b, and once negatively among the multiples of ab, and is thus reckoned once only. Again, each multiple of abc will appear among the $\frac{N}{a}$, $\frac{N}{b}$, $\frac{N}{c}$ terms which are multiples of a, b, c respectively; among the $\frac{N}{ab}$, $\frac{N}{ac}$, $\frac{N}{bc}$ terms which are multiples of ab, ac, bc respectively; and among the $\frac{N}{abc}$ multiples of abc; that is, since $3-3+1=1$, each multiple of abc occurs once, and once only. Similarly, other cases may be discussed.

433. [Wilson's Theorem.] *If* p *be a prime number*, $1+\lfloor\underline{p-1}$ *is divisible by* p.

By Ex. 2, Art. 314 we have

$$\lfloor\underline{p-1} = (p-1)^{p-1} - (p-1)(p-2)^{p-1} + \frac{(p-1)(p-2)}{1\,.\,2}(p-3)^{p-1} - \frac{(p-1)(p-2)(p-3)}{\lfloor\underline{3}}(p-4)^{p-1} + \ldots \text{ to } p-1 \text{ terms};$$

and by Fermat's Theorem each of the expressions $(p-1)^{p-1}$, $(p-2)^{p-1}$, $(p-3)^{p-1}$, ... is of the form $1+M(p)$; thus

$$\begin{aligned}\lfloor\underline{p-1} &= M(p) + \left\{1 - (p-1) + \frac{(p-1)(p-2)}{1\,.\,2} - \ldots \text{ to } p-1 \text{ terms}\right\}\\ &= M(p) + \{(1-1)^{p-1} - (-1)^{p-1}\}\\ &= M(p) - 1, \text{ since } p-1 \text{ is even.}\end{aligned}$$

Therefore $1+\lfloor\underline{p-1} = M(p)$.

This theorem is only true when p is prime. For suppose p has a factor q; then q is less than p and must divide $\lfloor\underline{p-1}$; hence $1+\lfloor\underline{p-1}$ is not a multiple of q, and therefore not a multiple of p.

Wilson's Theorem may also be proved without using the result quoted from Art. 314, as in the following article.

434. [Wilson's Theorem.] *If* p *be a prime number,* $1 + \lfloor\underline{p-1}$ *is divisible by* p.

Let a denote *any one* of the numbers

$$1,\ 2,\ 3,\ 4,\ \ldots\ (p-1)\ \ldots\ldots\ldots\ldots\ldots\ldots(1),$$

then a is prime to p, and if the products

$$1.a,\ 2.a,\ 3.a,\ \ldots\ldots\ (p-1)\,a$$

are divided by p, one and only one of them leaves the remainder 1. [Art. 426.]

Let this be the product ma; then we can shew that the numbers m and a are different unless $a = p-1$ or 1. For if a^2 were to give remainder 1 on division by p, we should have

$$a^2 - 1 \equiv 0 \pmod{p},$$

and since p is prime, this can only be the case when $a+1=p$, or $a-1=0$; that is, when $a=p-1$ or 1.

Hence one and only one of the products $2a$, $3a$, ... $(p-2)\,a$ gives remainder 1 when divided by p; that is, for *any one* of the series of numbers in (1), excluding the first and last, it is possible to find *one other*, such that the product of the pair is of the form $M(p)+1$.

Therefore the integers 2, 3, 4, ... $(p-2)$, the number of which is even, can be associated in pairs such that the product of each pair is of the form $M(p)+1$.

Therefore by multiplying all these pairs together, we have

$$2\,.\,3\,.\,4\ \ldots\ (p-2) = M(p)+1\,;$$

that is,
$$1\,.\,2\,.\,3\,.\,4\ \ldots\ (p-1) = (p-1)\,\{M(p)+1\}\,;$$

whence
$$\lfloor\underline{p-1} = M(p) + p - 1\,;$$

or $1 + \lfloor\underline{p-1}$ is a multiple of p.

Cor. If $2p+1$ is a prime number $\left(\lfloor\underline{p}\right)^2 + (-1)^p$ is divisible by $2p+1$.

For by Wilson's Theorem $1 + \lfloor\underline{2p}$ is divisible by $2p+1$. Put $n = 2p+1$, so that $p+1 = n-p$; then

$$\begin{aligned}\lfloor\underline{2p} &= 1\,.\,2\,.\,3\,.\,4\ \ldots\ldots\ p\,(p+1)\,(p+2)\ \ldots\ldots\ (n-1)\\ &= 1\,(n-1)\,2\,(n-2)\,3\,(n-3)\ \ldots\ p\,(n-p)\\ &= \text{a multiple of } n + (-1)^p\,(\lfloor\underline{p})^2.\end{aligned}$$

Therefore $1 + (-1)^p\,(\lfloor\underline{p})^2$ is divisible by n or $2p+1$, and therefore $(\lfloor\underline{p})^2 + (-1)^p$ is divisible by $2p+1$.

435. Many theorems relating to the properties of numbers can be proved by induction.

Example 1. If p is a prime number, $x^p - x$ is divisible by p.

Let $x^p - x$ be denoted by $f(x)$; then

$$\begin{aligned} f(x+1) - f(x) &= (x+1)^p - (x+1) - (x^p - x) \\ &= px^{p-1} + \frac{p(p-1)}{1 \cdot 2} x^{p-2} + \ldots + px \\ &= \text{a multiple of } p, \text{ if } p \text{ is prime [Art. 419.]} \\ \therefore f(x+1) &= f(x) + \text{a multiple of } p. \end{aligned}$$

If therefore $f(x)$ is divisible by p, so also is $f(x+1)$; but

$$f(2) = 2^p - 2 = (1+1)^p - 2,$$

and this is a multiple of p when p is prime [Art. 419]; therefore $f(3)$ is divisible by p, therefore $f(4)$ is divisible by p, and so on; thus the proposition is true universally.

This furnishes another proof of Fermat's theorem, for if x is prime to p, it follows that $x^{p-1} - 1$ is a multiple of p.

Example 2. Prove that $5^{2n+2} - 24n - 25$ is divisible by 576.

Let $5^{2n+2} - 24n - 25$ be denoted by $f(n)$;

then
$$\begin{aligned} f(n+1) &= 5^{2n+4} - 24(n+1) - 25 \\ &= 5^2 \cdot 5^{2n+2} - 24n - 49; \\ \therefore f(n+1) - 25 f(n) &= 25(24n+25) - 24n - 49 \\ &= 576(n+1). \end{aligned}$$

Therefore if $f(n)$ is divisible by 576, so also is $f(n+1)$; but by trial we see that the theorem is true when $n=1$, therefore it is true when $n=2$, therefore it is true when $n=3$, and so on; thus it is true universally.

The above result may also be proved as follows:

$$\begin{aligned} 5^{2n+2} - 24n - 25 &= 25^{n+1} - 24n - 25 \\ &= 25(1+24)^n - 24n - 25 \\ &= 25 + 25 \cdot n \cdot 24 + M(24^2) - 24n - 25 \\ &= 576n + M(576) \\ &= M(576). \end{aligned}$$

EXAMPLES. XXX. b.

1. Shew that $10^n + 3 \cdot 4^{n+2} + 5$ is divisible by 9.
2. Shew that $2 \cdot 7^n + 3 \cdot 5^n - 5$ is a multiple of 24.
3. Shew that $4 \cdot 6^n + 5^{n+1}$ when divided by 20 leaves remainder 9.
4. Shew that $8 \cdot 7^n + 4^{n+2}$ is of the form $24(2r-1)$.

5. If p is prime, shew that $2\lfloor\underline{p-3}+1$ is a multiple of p.

6. Shew that $a^{4b+1}-a$ is divisible by 30.

7. Shew that the highest power of 2 contained in $\lfloor\underline{2^r-1}$ is 2^r-r-1.

8. Shew that $3^{4n+2}+5^{2n+1}$ is a multiple of 14.

9. Shew that $3^{2n+5}+160n^2-56n-243$ is divisible by 512.

10. Prove that the sum of the coefficients of the odd powers of x in the expansion of $(1+x+x^2+x^3+x^4)^{n-1}$, when n is a prime number other than 5, is divisible by n.

11. If n is a prime number greater than 7, shew that n^6-1 is divisible by 504.

12. If n is an odd number, prove that $n^6+3n^4+7n^2-11$ is a multiple of 128.

13. If p is a prime number, shew that the coefficients of the terms of $(1+x)^{p-1}$ are alternately greater and less by unity than some multiple of p.

14. If p is a prime, shew that the sum of the $(p-1)^{\text{th}}$ powers of any p numbers in arithmetical progression, wherein the common difference is not divisible by p, is less by 1 than a multiple of p.

15. Shew that $a^{12}-b^{12}$ is divisible by 91, if a and b are both prime to 91.

16. If p is a prime, shew that $\lfloor\underline{p-2r}\,\lfloor\underline{2r-1}-1$ is divisible by p.

17. If $n-1$, $n+1$ are both prime numbers greater than 5, shew that $n(n^2-4)$ is divisible by 120, and $n^2(n^2+16)$ by 720. Also shew that n must be of the form $30t$ or $30t\pm12$.

18. Shew that the highest power of n which is contained in $\lfloor\underline{n^r-1}$ is equal to $\dfrac{n^r-nr+r-1}{n-1}$.

19. If p is a prime number, and a prime to p, and if a square number c^2 can be found such that c^2-a is divisible by p, shew that $a^{\frac{1}{2}(p-1)}-1$ is divisible by p.

20. Find the general solution of the congruence

$$98x-1\equiv0 \pmod{139}.$$

21. Shew that the sum of the squares of all the numbers less than a given number N and prime to it is

$$\frac{N^3}{3}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots.+\frac{N}{6}(1-a)(1-b)(1-c)\ldots,$$

and the sum of the cubes is

$$\frac{N^4}{4}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots.+\frac{N^2}{4}(1-a)(1-b)(1-c)\ldots,$$

$a, b, c\ldots$ being the different prime factors of N.

22. If p and q are any two positive integers, shew that $\lfloor\underline{pq}$ is divisible by $(\lfloor\underline{p})^q.\lfloor\underline{q}$ and by $(\lfloor\underline{q})^p.\lfloor\underline{p}$.

23. Shew that the square numbers which are also triangular are given by the squares of the coefficients of the powers of x in the expansion of $\dfrac{1}{1-6x+x^2}$, and that the square numbers which are also pentagonal by the coefficients of the powers of x in the expansion of

$$\frac{1}{1-10x+x^2}.$$

24. Shew that the sum of the fourth powers of all the numbers less than N and prime to it is

$$\frac{N^5}{5}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots.+\frac{N^3}{3}(1-a)(1-b)(1-b)\ldots$$
$$-\frac{N}{30}(1-a^3)(1-b^3)(1-c^3)\ldots,$$

$a, b, c,\ldots$ being the different prime factors of N.

25. If $\phi(N)$ is the number of integers which are less than N and prime to it, and if x is prime to N, shew that

$$x^{\phi(N)}-1\equiv 0 \pmod{N}.$$

26. If $d_1, d_2, d_3, \ldots$ denote the divisors of a number N, then

$$\phi(d_1)+\phi(d_2)+\phi(d_3)+\ldots=N.$$

Shew also that

$$\phi(1)\frac{x}{1+x^2}-\phi(3)\frac{x^3}{1+x^6}+\phi(5)\frac{x^5}{1+x^{10}}-\ldots \textit{ ad inf.}=\frac{x(1-x^2)}{(1+x^2)^2}.$$