Fundamental Theorem of Arithmetic

Some positive integers are prime numbers.

2, 3, 5, 7, 11, 13, 17, 19….

All the others can be written, in just one way, as a product of prime numbers. For example:

$60=6\times 10=2\times 3\times 2\times 5=(2^2)(3)(5)$

In general:

If N is any positive integer (except 1) then $N=(2^a)(3^b)(5^c)(7^d)(11^e)(...)$

where $a,b,c,...$ are zero or positive integers.

Example 1

Highest common factor (HCF) and Lowest common multiple (LCM)

the factors of 24 are:	1, 2, 3, 4, 6, 8, 12, 24
the factors of 30 are:	1, 2, 3, 5, 6, 10, 15, 30
the common factors of 24 and 30 are:	1, 2, 3, 6

So $HCF(24{,}30)=6$

the multiples of 24 are:	24, 48, 72, 96, 120, 144, 168, 192, 216, 240, 264 ...
the multiples of 30 are:	30, 60, 90, 120, 150, 180, 210, 240, 270, 300, 330 ...
the common multiples of 24 and 30 are:	120, 240, ...

So $LCM(24{,}30)=120$

Example 2

$A=(2^5)(3^1)(5^0)(7^6)(11^2)$ and $B=(2^3)(3^7)(5^4)(7^8)(11^0)$

2^5 is a factor of A and 2^3 is a factor of B so HCF is a multiple of 2^3

3^1 is a factor of A and 3^7 is a factor of B so HCF is a multiple of 3^1

etc

So $HCF(A,B)=(2^3)(3^1)(5^0)(7^6)(11^0)$

A is a multiple of 2^5 and B is a multiple of 2^3 so LCM is a multiple of 2^5

A is a multiple of 3^1 and B is a multiple of 3^7 so LCM is a multiple of 3^7

etc

So $LCM(A,B)=(2^5)(3^7)(5^4)(7^8)(11^2)$

note

$HCF(A,B)\times LCM(A,B)=(2^8)(3^8)(5^4)(7^{14})(11^2)=AB$

Example 3

$N=(2^a)(3^b)(5^c)(7^d)(11^e)(...)$

If N is a multiple of 5 then $c\geq 1$ If N is not a multiple of 5 then $c=0$

If N is a multiple of 3 and a multiple of 7 then $b\geq 1$ and $d\geq 1$
So N is a multiple of 21

If N is a multiple of 6 then N is a multiple of 2 and a multiple of 3 so $a\geq 1$ and $b\geq 1$
If N is a multiple of 15 then N is a multiple of 3 and a multiple of 5 so $b\geq 1$ and $c\geq 1$
So if N is a multiple of 6 and a multiple of 15 then N must be a multiple of 30

In general:
If N is a multiple of a and a multiple of b then N is a multiple of $LCM(a,b)$

Example 4

$N=(2)(3^2)(13^4)$ $M=(5^3)(7^5)(13)(23)$ so $NM=(2)(3^2)(5^3)(7^5)(13^5)(23)$

NM is a multiple of 3 because N is a multiple of 3

NM is a multiple of 7 because M is a multiple of 7

NM is not a multiple of 17 because neither N nor M is a multiple of 17

but:

NM is a multiple of 14 even though neither N nor M is a multiple of 14

this is because $14=2\times 7$ and N is a multiple of 2 and M is a multiple of 7

also:

NM is a multiple of 35 but N and 35 have no common factor. So all the factors of 35 must appear in M So M must be a multiple of 35

In general: if p is prime:

NM is a multiple of p only if N or M (or both) is a multiple of p

In general: if N and r have no common factor:

NM is a multiple of r only if M is a multiple of r

see Exercise 1

Theorem

$\sqrt{2}$ is irrational

Proof (by contradiction)

Assume $\sqrt{2}$ is rational

So:

$\sqrt{2}=\frac{p}{q}$ where p and q are positive integers

So:

$2q^2=p^2$

Now:

We can write q as a product of primes:

$q=(2^a)(3^b)(5^c)(7^d)(11^e)(...)$

So:

$q^2=(2^{2a})(3^{2b})(5^{2c})(7^{2d})(11^{2e})(...)$ the powers of all the primes are even

So:

$2q^2=(2^{2a+1})(3^{2b})(5^{2c})(7^{2d})(11^{2e})(...)$ the power of 2 is odd

Now:

We can write p as a product of primes:

$p=\ldots$

So:

$p^2=\ldots$ all the powers of all the primes are even

But:

$2q^2=p^2$

LHS, power of 2 is odd. RHS, power of 2 is even.

Contradiction.

There is another proof that $\sqrt{2}$ is irrational in the chapter: Proof by Contradiction

But this proof is better, because it suggests why the result is true and it suggests further results.

See Exercise 2

EXERCISE 1

1) Write 5619250 in the form $(2^a)(3^b)(5^c)(7^d)(11^e)(...)$

2) Find $HCF(36652,38698)$ and $LCM(36652,38698)$

3) $532400=(2^4)(5^2)(11^3)$ How many factors has 532400 got?

4) This question is difficult

a) If n^2 is a multiple of 7 show that n is a multiple of 7

b) If n^2 is a multiple of 6 show that n is a multiple of 6

c) If n^2 is a multiple of 12 show that n might not be a multiple of 12

d) For what values of m is the following true:

If n^2 is a multiple of m then n must be a multiple of m ?

EXERCISE 2

1) Prove $5^{1/3}$ is irrational

2) What happens when we try to prove $\sqrt{4}$ is irrational?

SOLUTIONS 1

1) $5619250=(2)(5^3)(7)(13^2)(19)$

2) $36652=(2^2)(7^2)(11^1)(17^1)$ and $38698=(2^1)(11^1)(1759^1)$

$HCF(36652,38698)=(2^1)(11^1)=22$

$LCM(36652,38698)=(2^2)(7^2)(11^1)(17^1)(1759^1)=64470868$

3) $532400=(2^4)(5^2)(11^3)$ so any factor can be written as $(2^p)(5^q)(11^r)$

where $p=0,1,2,3,4$ and $q=0,1,2$ and $r=0,1,2,3$

We have 5 choices for the value of p and 3 choices for the value of q and 4 choices for the value of r So there are $5\times3\times4=60$ choices for p,q,r

So 532400 has 60 factors (including 1 and 532400)

4) $n=(2^a)(3^b)(5^c)(7^d)(11^e)(...)$

$n^2=(2^{2a})(3^{2b})(5^{2c})(7^{2d})(11^{2e})(...)$

proof by contrapositive

a) If n is not a multiple of 7 then $d=0$ and n^2 is not a multiple of 7

b) If n is not a multiple of 6 then $a=0$ or $b=0$ and n^2 is not a multiple of 6

c) If n is not a multiple of 12 then we cannot say $a=0$ or $b=0$ because we could have $a=1$ and $b=1$ for example if $n=6$

6^2 is a multiple of 12 but 6 is not a multiple of 12

d) $m=(2^a)(3^b)(5^c)(7^d)(11^e)(...)$

The statement is true if $a=0,1$ $b=0,1$ $c=0,1$ etc

SOLUTIONS 2

1) Assume $5^{1/3}$ is rational

$5^{1/3}=\frac{p}{q}$ where p and q are integers

$5q^3=p^3$

We can write q as a product of powers of primes:

$q=(2^a)(3^b)(5^c)(7^d)(11^e)(...)$

$q^3=(2^{3a})(3^{3b})(5^{3c})(7^{3d})(11^{3e})(...)$ all the powers of all the primes are multiples of three.

$5q^3=(2^{3a})(3^{3b})(5^{3c+1})(7^{3d})(11^{3e})(...)$ the power of 5 is not a multiple of three.

We can write p as a product of powers of primes:

$p=\ldots$

$p^3=\ldots$ all the powers of all the primes are multiples of three

$5q^3=p^3$

LHS, power of 5 is not a multiple of three. RHS, power of 5 is a multiple of three.

Contradiction.

2) Claim

$\sqrt{4}$ is irrational

Attempted proof (by contradiction)

Assume $\sqrt{4}$ is rational

$\sqrt{4}=\frac{p}{q}$ where p and q are positive integers

$4q^2=p^2$

We can write q as a product of primes:

$q=(2^a)(3^b)(5^c)(7^d)(11^e)(...)$

$q^2=(2^{2a})(3^{2b})(5^{2c})(7^{2d})(11^{2e})(...)$ the powers of all the primes are even

$4q^2=(2^{2a+2})(3^{2b})(5^{2c})(7^{2d})(11^{2e})(...)$ the power of 2 is still even!

This is where our proof falls apart.

Euclid’s Algorithm

An algorithm is a set of precise instructions that will solve a problem. Euclid’s algorithm will solve the problem of finding the highest common factor of two positive integers.

Here is Euclid’s algorithm for finding $HCF(3458,651)$

$d=HCF(3458,651)$

We divide 3458 by 651

$3458=(5)(651)+203$

If 3458 and 651 are both multiples of d then 651 and 203 are both multiples of d

We now repeat the procedure:

$651=(3)(203)+42$

If 651 and 203 are both multiples of d then 203 and 42 are both multiples of d

$203=(4)(42)+35$

If 203 and 42 are both multiples of d then 42 and 35 are both multiples of d

$42=(1)(35)+7$

If 42 and 35 are both multiples of d then 35 and 7 are both multiples of d

$35=(5)(7)+0$ STOP

So $d=7$

See Exercise 1

We can now write HCF(3458,651) in the form $3458n+65m$ for integers n and m

Working back up the page:

$7=(42)+(-1)(35)$ But $35=203+(-4)(42)$

$7=(-1)(203)+(5)(42)$ But $42=651+(-3)(203)$

$7=(5)(651)+(-16)(203)$ But $203=3458+(-5)(651)$

$7=(-16)(3458)+(85)(651)$

We can use Euclid’s algorithm to solve some Diophantine equations. A Diophantine equation requires integer solutions.

Example

Solve $3458x+651y=47894$ where x,y are integers

Run Euclid’s algorithm to find $HCF(3458,651)$

We have just done this and we found:

$HCF(3458, 651) = 7$

Then we found:

$7 = (-16)(3458) + (85)(651)$ so $(3458)(-16) + (651)(85) = 7$

Now $\frac{47894}{7} = 6842$ so we multiply both sides by 6842

So:

$(3458)(-109472) + (651)(581570) = 47894$

We have a solution to our equation: $x = -109472$ $y = 581570$

There are more solutions. The general solution is:

$x = -109472 + 93t$ and $y = 581570 - 494t$ for any integer t Can you see why?

See exercise 2

EXERCISE 1

Find the highest common factor of 41325 and 5814

SOLUTION 1

$41325 = (7)(5814) + (627)$

$5814 = (9)(627) + (171)$

$627 = (3)(171) + (114)$

$171 = (1)(114) + (57)$

$114 = (2)(57) + (0)$ STOP

$d = 57$

EXERCISE 2

1) Oranges cost 23p and apples cost 17p. I buy some and the cost is 549p

How many oranges and how many apples did I buy?

Hint: If I buy x oranges and y apples then $23x + 17y = 549$

2) In the following equations, we are looking for solutions where x, y are integers.

Why won’t we find any?

a) $7x = 43$ b) $(x-3)^2 = 10$ c) $4x = 2y + 1$ d) $2^x = 3^y$

e) $6^x = 10^y$

SOLUTIONS 2

1) $23=(1)(17)+(6)$

$17=(2)(6)+(5)$

$6=(1)(5)+(1)$

$5=(5)(1)+0$ STOP

$d=1$ (this was obvious as 23 and 17 are primes)

Working back up the page

$1=(6)+(-1)(5)$ But $(5)=(17)+(-2)(6)$

$1=(-1)(17)+(3)(6)$ But $(6)=(23)+(-1)(17)$

$1=(3)(23)+(-4)(17)$

So $(23)(3)+(17)(-4)=1$ multiplying by 549 gives

$(23)(1647)+(17)(-2196)=549$

We have a solution to our equation $x=1647$ and $y=-2196$

So I buy 1647 oranges and -2196 apples

This is not a very practical solution.

The general solution is: $x=1647-17t$ and $y=-2196+23t$

We want $1647-17t\geq 0$ and $-2196+23t\geq 0$

So $t\leq 96.9$ and $t\geq 95.5$ and remember t is an integer, so $t=96$

This gives $x=15$ and $y=12$

2)

a) LHS is a multiple of 7 but RHS is not a multiple of 7

b) No integer squared is equal to 10

c) LHS is even but RHS is odd

d) LHS is even but RHS is odd

e) LHS is a multiple of 3 but the RHS is not a multiple of 3

Prime Numbers

Theorems about prime numbers:

1. Euclid’s theorem

There are an infinite number of prime numbers

Proof

Eric says $2,3,5,7,11$ is a list of all the prime numbers.

But consider the number $N=(2\times3\times5\times7\times11)+1$

If N is prime, then Eric’s list is not complete.

If N is not prime, then it is a multiple of primes. But N is not a multiple of 2, 3, 5, 7 or 11 so N is a multiple of some other primes. So Eric’s list is not complete.

We can repeat this argument for any list that Eric can come up with. So it is impossible to write down a list of all the primes. So there must be an infinite number of primes.

2. We can find an arbitrarily long sequence of consecutive non-primes.

Proof

$6!$ is a multiple of 2, so $2+6!$ is a multiple of 2.

$6!$ is a multiple of 3, so $3+6!$ is a multiple of 3

...

$6!$ is a multiple of 6, so $6+6!$ is a multiple of 6

So we have found a sequence of 5 consecutive non-primes.

In general:

$(2+n!),(3+n!),(4+n!),...(n+n!)$ is a sequence of $n-1$ consecutive non-primes for any positive integer n

3. We cannot find an arithmetic sequence where all the terms are primes.

Proof

Here is an arithmetic sequence: $7,157,307,457,607,757,907\ldots$

The first seven terms are all primes.

Now:

$a=7$ and $d=150$ and $u_n=7+(n-1)150$

So:

$u_8=7+(7)150$ and this is a multiple of 7 and therefore not a prime.

In general:

Consider the arithmetic sequence; $a,a+d,a+2d,a+3d,\ldots$

Now:

$u_n=a+(n-1)d$ so $u_{a+1}=a+ad$ and this is a multiple of a and therefore not prime.

Note:

if $a=1$ our proof does not work but if $a=1$ then the first term of the arithmetic sequence is not prime.

Dirichlet’s theorem:

If a and d have no common factor then the arithmetic sequence $a,a+d,a+2d,a+3d,\ldots$ will contain an infinite number of primes.

So the terms of $7,157,307,457,607,757,907\ldots$ cannot all be prime, only an infinite number of them.

It is difficult to prove Dirichlet’s theorem but we can prove that there are an infinite number of primes in the arithmetic sequence:

$5,9,13,17,21,23,\ldots$

These are the integers of the form $4k+3$

So we want to prove that there are an infinite number of primes of the form $4k+3$

Before we start the proof:

All primes (except 2) are of the form $4k+1$ or $4k+3$

The product of primes of the form $4k+1$ is also of this form because:

$(4k+1)(4q+1)=\ldots=4(4kq+k+q)+1$

Proof

Eric says $3,7,11,19,23$ is a list of all the $4k+3$ primes.

But consider the number $N=4(3\times7\times11\times19\times23)+3$

N is of the form $4k+3$

If N is prime, then Eric’s list is not complete.

If N is not prime, then it is a multiple of primes. But N is not a multiple of 3, 7, 11, 19 or 23 so N is a multiple of some other primes. If these other primes were all of the form $4k+1$ then N would be of the form $4k+1$ as we saw above. So at least one of these other primes must be of the form $4k+3$ So Eric’s list is not complete.

We can repeat this argument for any list that Eric can come up with. So it is impossible to write down a list of all the $4k+3$ primes. So there must be an infinite number of $4k+3$ primes.

4.

$f(n)=n^2-n+41$ is prime for $n=1,2,3,\ldots 40$

and

$f(n)=n^2-79n+1601$ is prime for $n=1,2,3,\ldots 79$

But:

No quadratic polynomial $f(n)$ with integer coefficients, is prime for all values of n

Proof

$f(n)=an^2+bn+c$ where a,b,c are integers

$f(1)=a+b+c$ let $q=a+b+c$

$f(q+1)=a(q+1)^2+b(q+1)+c=\ldots=q(aq+2a+b+1)$

If $q=0$ then $f(1)=0$ and therefore not a prime.

If $q=1$ then $f(1)=1$ and therefore not a prime.

If $q\geq 2$ then $f(q+1)$ is a multiple of q and therefore not a prime.

In general:

No polynomial $f(n)$ with integer coefficients, is prime for all values of n

5. For every integer $n\geq 1$ there is a prime p where $n\leq p\leq 2n$

Proof – too difficult

6. x and n are positive integers

If x^n-1 is prime then $x=2$

For example, when $n=5$

$x^5-1=(x-1)(x^4+x^3+x^2+x+1)$

So $(x-1)$ is a factor of (x^5-1) so (x^5-1) cannot be prime unless $(x-1)=1$ so $x=2$

So we can see that if $x\neq 2$ then x^n-1 is not prime.

Note: This does not mean, if $x=2$ then x^n-1 is prime - try $n=4$

7. n is a positive integer

If 2^n-1 is prime then n is prime.

For example, when $n=15$

$2^{15}-1=(2^3)^5-1=8^5-1$ and this is not prime by theorem 6.

So we can see that if n is not prime then 2^n-1 is not prime.

Note: This does not mean, if n is prime then $2^n - 1$ is prime - try $n=11$

Primes of the form $2^n - 1$ are called Mersenne primes.
Some people like looking for large primes. Many of these are Mersenne primes, such as $2^{82589933} - 1$ because there are short cuts to check if numbers of the form $2^n - 1$ are prime, such as the Lucas – Lehmer test (look it up!)

8. x and n are positive integers
If $x^n + 1$ is prime then n is even

For example, when $n=5$

$$x^5 + 1 = (x+1)(x^4 - x^3 + x^2 - x + 1)$$

So (x+1) is a factor of $(x^5 + 1)$ so $(x^5 + 1)$ cannot be prime.
So we can see that if n is odd then $x^n + 1$ is not prime.

Note: This does not mean, if n is even then $x^n + 1$ is prime – try $x=3$ and $n=2$

9. n is a positive integer
If $2^n + 1$ is prime then $n = 2^k$ for some positive integer k

For example, when $n=28$

$2^{28} + 1 = (2^4)^7 + 1 = 16^7 + 1$ and this cannot be prime by theorem 8.

So we can see that if $n \neq 2^k$ then $2^n + 1$ is not prime.

Note: this does not mean, if $n = 2^k$ then $2^n + 1$ is prime – try $n=32$

Numbers of the form $2^n + 1$ where $n = 2^k$ are called Fermat numbers.

The first five Fermat numbers are all prime but the sixth Fermat number is 4,294,967,297 and Euler showed that this is not prime. In fact, no other Fermat primes have been discovered.

Conjectures about primes:
1. There are an infinite number of Mersenne primes.
2. There are an infinite number of Fermat primes.

3. There are an infinite number of Fibonacci primes.

4. There are an infinite number of prime pairs (primes like 17 and 19 that differ by 2).

5. For every positive integer n there is a prime p where $n^2 < p < (n+1)^2$

6. There are infinitely many primes of the form n^2+1 where n is a positive integer

7. $2^k - 2$ is a multiple of k if and only if k is a prime number.

Actually this is not a conjecture. The statement is true for $k = 1, 2, 3, 4, \ldots 340$ but not for $k = 341$

8. The Goldbach conjecture

Every even integer, greater than 4, is the sum of two odd primes.

$6 = 3+3$ $8 = 3+5$ $10 = 3+7$ etc

This is the most famous conjectures about primes. It arose in a letter Goldbach wrote to Euler in 1742. In 1931, Schnirelmann proved that every even integer, greater than 4, is the sum of no more than 300,000 primes, which is a start.

Incidently, Goldbach had another conjecture:

Every odd positive integer, greater than 1, is a prime or the sum of a prime and twice a square.

$9 = 7+2(1^2)$ $15 = 7+2(2^2)$ $21 = 3+2(3^2)$ $25 = 7+2(3^2)$ etc

We now know that this conjecture is false. The smallest counter-example is 5777.

Modulo Arithmetic

Let’s write the integers $0,1,2,3,4,5,6,7...$ in four columns:

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15
16	17	18	19
20	21	22	23
…	…	…	…

If n is in the 0 column then:

$n=4k$ for some integer k for example $12=(4\times 3)$

n has remainder 0 when divided by 4

we say that $n=0, mod\ 4$

If n is in the 1 column then:

$n=4k+1$ for some integer k for example $21=(4\times 5)+1$

n has remainder 1 when divided by 4

we say that $n=1, mod\ 4$

If n is in the 2 column then:

$n=4k+2$ for some integer k for example $14=(4\times 3)+2$

n has remainder 2 when divided by 4

we say that $n=2, mod\ 4$

If n is in the 3 column then:

$n=4k+3$ for some integer k for example $7=(4\times 1)+3$

n has remainder 3 when divided by 4

we say that $n=3, mod\ 4$

If n and m are both in the r column then:

$n=4s+r$ and $m=4t+r$ for some integers s and t

n and m both have remainder r when divided by 4

$n-m$ is a multiple of 4

$n=m+4k$ for some integer k

we say that $n=m, mod 4$

I don't want to keep writing mod 4 so here is a shorthand. If you see:

mod 4:

…

end of mod 4

then everything in-between "mod 4" and "end of mod 4" will be in mod 4.

for example

mod 4:

$16=0$ $13=1$ $22=2$ $15=3$

$20=12$ $17=9$ $22=6$ $23=19$

end of mod 4

Looks weird but you'll get the hang of it.

mod 4:

$23=7$ and $13=5$

Check the following:

$23+13=7+5$

$23-13=7-5$

$23\times13=7\times5$

$23^2=7^2$

$23+147=13+147$

$147\times23=147\times13$

end of mod 4

In general:

mod 4:

If $a=A$ and $b=B$ then the following six rules apply:

rule 1 $a+b=A+B$

rule 2 $a-b=A-B$

rule 3 $ab = AB$

rule 4 $a^n = A^n$ for any integer n

rule 5 $a+n = A+n$ for any integer n

rule 6 $na = nA$ for any integer n

end of mod 4

Proof of rule 1

$a = A, mod\,4$ so $a = A+4k$ for some integer k

$b = B, mod\,4$ so $b = B+4l$ for some integer l

$a+b = (A+4k)+(B+4l) = (A+B)+4(k+l)$ So $a+b = A+B, mod\,4$

You can prove rules 2 to 6 in the same way.

What about division?

rule 7 – the cancellation rule

If $3p = 3q, mod\,4$ then $3p = 3q+4k$ for some integer k

So $3p-3q = 4k$ so $3(p-q) = 4k$ so $3(p-q)$ is a multiple of 4

In the chapter: Fundamental Theorem of Arithmetic we saw that:

If n and r have no common factor then:

nm is a multiple of r only if m is a multiple of r

3 and 4 have no common factor so:

$3m$ is a multiple of 4 only if m is a multiple of 4

Now $3(p-q)$ is a multiple of 4 so $(p-q)$ is a multiple of 4

So $p = q, mod\,4$

mod 4:

In general:

If $np = nq$ then $p = q$ provided n and 4 have no common factor.

This is the nearest we are going to get to doing division.

$15 = 39$

we can divide both sides by 3 (note: 3 and 4 do not have a common factor)

$5 = 13$

But

$10 = 34$

we cannot divide both sides by 2 (note: 2 and 4 do have a common factor)

$5\neq 17$

end of mod 4

We must be careful and stick to our 7 rules.

For example $5^2=7^2$ but $5\neq 7$ etc

We can extend these ideas to include negative integers

for example, $-17=-20+3=(4\times -5)+3=3, mod\, 4$

Everything we have said about mod 4 applies to mod 2, mod 3 etc

So what is the point of all this? Well, it can make proving some results a lot easier.

Example 1

No square is of the form $3k+2$

Proof

mod 3:

$x=0,1,2$ so $x^2=0,1$ so $x^2\neq 2$

end of mod 3

Get it? Here is some more explanation:

$x=0,1,2$ means that if x is any integer then:

$x=0, mod\, 3$ or $x=1, mod\, 3$ or $x=2, mod\, 3$

If $x=0, mod\, 3$ then $x^2=0^2=0, mod\, 3$

If $x=1, mod\, 3$ then $x^2=1^2=1, mod\, 3$

If $x=2, mod\, 3$ then $x^2=2^2=4=1, mod\, 3$

So $x^2=0, mod\, 3$ or $x^2=1, mod\, 3$

So

$x^2\neq 2, mod\, 3$ so x^2 cannot be of the form $3k+2$

Example 2

Show that the last digit of a square cannot be 2, 3, 7 or 8

Before we do the proof ...

for any positive integer, say 127, we can write:

$127=120+7=(10\times 12)+7=7, mod\, 10$

In general

mod 10:

$n=last\ digit\ of\ n$

end of mod 10

Proof

mod 10:

$x=0,1,2,3,4,5,6,7,8,9$ so $x^2=0,1,4,5,6,9$ so $x^2\neq 2,3,7,8$

end of mod 10

Example 3

No integer of the form $4k+2$ is the difference of two squares.

Proof

mod 4:

$a=0,1,2,3$ so $a^2=0,1$ and $b=0,1,2,3$ so $b^2=0,1$ so $a^2-b^2=0,1,3$ so $a^2-b^2\neq 2$

end of mod 4

see Exercise

If you don’t think that mod arithmetic is a brilliant idea, then do this Exercise without it.

EXERCISE

Show that:

1. No square is of the form $4k+2$ or $4k+3$ Hint: mod 4

2. Every odd square is of the form $8k+1$ Hint: mod 8

3. If x and y are odd integers then x^2-y^2 is a multiple of 8 Hint: see(2)

4. No even square is the sum of two odd squares Hint: mod 4

5. The sum of two consecutive squares is one more than a multiple of 4 Hint: mod 4

6. Every cube is of the form $9k$ $9k+1$ or $9k+8$ Hint: mod 9

7. The sum of three consecutive cubes is a multiple of 9. Hint: mod 9

8. The sum of 3 squares cannot be of the form $8k+7$ Hint: mod 8

9. No cube is of the form $4k+2$ Hint: mod 4

10. $x^4+y^4=z^4+4$ has no integer solution. Hint: mod 8

11. x^3-x is a multiple of 6 for any integer x Hint: mod 6

12. If x is an integer and not a multiple of 2 or 3 then x^2-1 is a multiple of 24

Hint: mod 24

13. If p is a prime greater than 3 then p^2+2 is a multiple of 3 Hint: mod 3

14. Every prime (except 2 and 3) is of the form $6k+1$ or $6k+5$ Hint: mod 6

SOLUTIONS

1) mod 4:

$x=0,1,2,3$ so $x^2=0,1$ so $x^2 \neq 2,3$

end of mod 4

2) mod 8:

if x is odd then $x=1,3,5,7$ so $x^2=1$

end of mod 8

3) mod 8:

if x is odd then $x=1,3,5,7$ so $x^2=1$

if y is odd then $y=1,3,5,7$ so $y^2=1$

so $x^2-y^2=0$

end of mod 8

4) mod 4:

if x is even then $x=0,2$ so $x^2=0$

if y is odd then $y=1,3$ so $y^2=1$

if z is odd then $z=1,3$ so $z^2=1$

so $x^2 \neq y^2+z^2$

end of mod 4

5) mod 4:

x	0	1	2	3
y	1	2	3	0
x^2	0	1	0	1
y^2	1	0	1	0
x^2+y^2	1	1	1	1

end of mod 4

6) mod 9:

$x=0,1,2,3,4,5,6,7,8$ so $x^3=0,1,8$

end of mod 9

7) mod 9:

x	0	1	2	3	4	5	6	7	8
y	1	2	3	4	5	6	7	8	0
z	2	3	4	5	6	7	8	0	1
x^3	0	1	8	0	1	8	0	1	8
y^3	1	8	0	1	8	0	1	8	0
z^3	8	0	1	8	0	1	8	0	1
$x^3+y^3+z^3$	9	9	9	9	9	9	9	9	9

end of mod 9

8) mod 8:

$x=0,1,2,3,4,5,6,7$ so $x^2=0,1,4$

$y=0,1,2,3,4,5,6,7$ so $y^2=0,1,4$

$z=0,1,2,3,4,5,6,7$ so $z^2=0,1,4$

$x^2+y^2+z^2=0,1,2,3,4,5,6$ so $x^2+y^2+z^2\neq 7$

end of mod 8

9) mod 4:

$x=0,1,2,3$ so $x^3=0,1,3$ so $x^3\neq 2$

end of mod 4

10) mod 8:

$x=0,1,2,3,4,5,6,7$ so $x^4=0,1$

$y=0,1,2,3,4,5,6,7$ so $y^4=0,1$

$x^4+y^4=0,1,2$

$z=0,1,2,3,4,5,6,7$ so $z^4=0,1$ so $z^4+4=5,6$

so $x^4+y^4\neq z^4+4$

end of mod 8

11) mod 6

x	0	1	2	3	4	5
x^3	0	1	2	3	4	5

$x^3-x=0$

end of mod 6

12) mod 24:

if x is not a multiple of 2 or 3 then $x=1,5,7,11,13,17,19,23$ so $x^2=1$ so $x^2-1=0$

end of mod 24

13) mod 3:

if p is a prime greater than 3 then $p=1,2$ so $p^2=1$ so $p^2+2=3=0$

end of mod 3

14)

p is a prime greater than 3

if $p=0,mod\,6$ then p is a multiple of 6

if $p=2,mod\,6$ then p is a multiple of 2

if $p=3,mod\,6$ then p is a multiple of 3

if $p=4,mod\,6$ then p is a multiple of 2

so $p=1,5,mod\,6$

Chinese Remainder Theorem

I have a large bag of sweets. If I share them equally among my 10 children there are 2 sweets left over. If I share them equally among my 7 grandchildren there are 3 sweets left over. How many sweets are in my bag?

If there are x sweets in the bag then $x=2, mod\,10$ and $x=3, mod\,7$

Theorem

This problem has a unique solution for $x=1,2,\ldots 70$

Proof (by contradiction)

Assume there are two solutions $x=p$ and $x=q$

$p=2, mod\,10$ $p=3, mod\,7$

$q=2, mod\,10$ $q=3, mod\,7$

Say $p>q$

$p=2, mod\,10$ $q=2, mod\,10$

So $p=q+10m$ for some positive integer m

$p=3, mod\,7$ $q=3, mod\,7$

So $p=q+7n$ for some positive integer n

So $q+10m=q+7n$ so $10m=7n$

So $10m$ is a multiple of 7

But 10 and 7 have no common factor so m is a multiple of 7

So $m=7k$ for some positive integer k

So:

$p=q+10m$ $m=7k$

So $p=q+70k$

But:

$1\le p\le 70$ $1\le q\le 70$

Contradiction!

In general:

The simultaneous equations:

$x=a, mod\,m$ $x=b, mod\,n$ where m and n have no common factor have a unique solution for $x=1,2,...mn$

A tedious method to find this solution:

$x=2, mod\,10$ so $x=2,12,22,32,42,52,62$

$x=3, mod\,7$ so $x=3,10,17,24,31,38,45,52,59,66$

This gives the solution $x=52$

Note:

The smallest number of sweets I could have in my bag is 52.

But I could have $52+70L$ sweets in my bag where L is any positive integer.

Can you see why?

Fermat’s Last Theorem

A primitive Pythagorean triple is a set of three positive integers x, y, z where:

$x^2+y^2=z^2$ and x, y, z have no common factor.

for example:

$5, 12, 13$

Theorem

All primitive Pythagorean triples are of the form:

$x=2pq \qquad y=p^2-q^2 \qquad z=p^2+q^2$

where p and q are any positive integers such that:

$p>q$

p and q have no common factor

p and q are not both odd

p and q are not both even

for example $p=7$ and $q=4$ gives $x=56 \quad y=33 \quad z=65$

Proof(?)

We can easily check that:

$(2pq)^2+(p^2-q^2)^2=(p^2+q^2)^2$

But this does not prove that all primitive Pythagorean triples are of this form. Why not?

See Exercise

Fermat’s Last Theorem:

There is no set of three positive integers x, y, z where:

$x^3+y^3=z^3$ or $x^4+y^4=z^4$ or $x^5+y^5=z^5$ ...etc

Fermat had the annoying habit of announcing theorems that he had discovered but not providing proofs. It was left to later mathematicians (Euler usually) to supply the proofs. Fermat’s last theorem (1637) was the last of these theorems to be proved (1995)

EXERCISE

Prove the following about primitive Pythagorean triples.

1) x and y can’t both be even hint: mod 2

2) x and y can’t both be odd hint: mod 4

3) z is odd

4) x or y is a multiple of 3 hint: mod 3

5) x or y is a multiple of 4 hint: mod 16

6) x or y or z is a multiple of 5 hint: mod 5

7) xyz is a multiple of 60

SOLUTIONS

1) proof by contradiction

assume x and y are both even

mod 2:

$x=0$ so $x^2=0$

$y=0$ so $y^2=0$

$x^2+y^2=z^2$ so $z^2=0$ so $z=0$ so x,y,z are all even so x,y,z have a common factor

Contradiction

end of mod 2

2) proof by contradiction

assume x and y are both odd

mod 4:

$x=1,3$ so $x^2=1$

$y=1,3$ so $y^2=1$

$x^2+y^2=z^2$ so $z^2=2$ but if $z=0,1,2,3$ then $z^2=0,1$

Contradiction

end of mod 4

3) parts (1) and (2) tell us that x^2+y^2 is odd so z^2 is odd so z is odd

4) proof by contradiction

assume neither x nor y is a multiple of 3

mod 3:

$x=1,2$ so $x^2=1$

$y=1,2$ so $y^2=1$

$x^2+y^2=z^2$ so $z^2=2$ but if $z=0,1,2$ then $z^2=0,1$

Contradiction

end of mod 3

5) proof by contradiction

assume neither x nor y is a multiple of 4

mod 16:

$x=1,2,3,5,6,7,9,10,11,13,14,15$ so $x^2=1,4,9$

$y=1,2,3,5,6,7,9,10,11,13,14,15$ so $y^2=1,4,9$

$x^2+y^2=z^2$ so $z^2=2,5,8,10,13$

but if $Z=0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15$ then $z^2=0,1,4,9$

Contradiction

end of mod 16

6) proof by contradiction

assume neither x nor y nor z is a multiple of 5

mod 5:

$x=1,2,3,4$ so $x^2=1,4$

$y=1,2,3,4$ so $y^2=1,4$

$x^2+y^2=z^2$ so $z^2=0,2,3$ but if $z=1,2,3,4$ then $z^2=1,4$

Contradiction

end of mod 5

7) this follows from parts (4), (5) and (6)

Fermat’s Little Theorem

Theorem

$n^7 - n$ is a multiple of 7, for $n=1,2,3,\dots$

for example $153^7 - 153$ is a multiple of 7

Proof (by induction)

part 1:

If $n=1$ then $n^7 - n = 0$

So $n^7 - n$ is a multiple of 7 when $n=1$

part 2:

If $n^7 - n$ is a multiple of 7 when $n=k$ then:

$k^7 - k$ is a multiple of 7, so $k^7 - k = 7r$ for some integer r

Now $(k+1)^7 - (k+1) = (k^7 + 7k^6 + 21k^5 + 35k^4 + 35k^3 + 21k^2 + 7k + 1) - (k+1)$

So $(k+1)^7 - (k+1) = (k^7 - k) + (7k^6 + 21k^5 + 35k^4 + 35k^3 + 21k^2 + 7k)$

So $(k+1)^7 - (k+1) = 7r + 7(k^6 + 3k^5 + 5k^4 + 5k^3 + 3k^2 + k)$

So $(k+1)^7 - (k+1)$ is a multiple of 7

So $n^7 - n$ is a multiple of 7 when $n = k+1$

Note: our proof worked because the coefficients in the binomial theorem: $7, 21, 35, 35, 21, 7$ are all multiples of 7

A typical coefficient is: $(7C3) = \dfrac{7\times6\times5\times4\times3\times2\times1}{(3\times2\times1)(4\times3\times2\times1)}$

After lots of cancelling, we are left with a positive integer. The 7 on the top of the fraction can’t be cancelled out by numbers on the bottom of the fraction because 7 is prime. So $(7C3)$ must be a multiple of 7

In general:

If p is prime then all the coefficients in the expansion of $(k+1)^p$ will be a multiple of p (apart from the 1’s at each end)

In general:

Fermat’s Little Theorem (FLT) for prime number p and $n=1,2,3,\dots$

$n^p - n$ is a multiple of p

We can prove this for prime number p as we proved it above for prime number 7

Now:

$n^7 - n$ is a multiple of 7, so $n(n^6 - 1)$ is a multiple of 7

So:

if n is not a multiple of 7 then $n^6 - 1$ is a multiple of 7

So we can rephrase:

Fermat's Little Theorem (FLT) for prime number p and $n = 1, 2, 3, \ldots$

$n^{(p-1)} - 1$ is a multiple of p provided n is not a multiple of p

We can rephrase using mod arithmetic:

Fermat's Little Theorem (FLT) for prime number p and $n = 1, 2, 3, \ldots$

$n^p - n = 0, mod\, p$ so $n^p = n, mod\, p$

Or:

$n^{(p-1)} - 1 = 0, mod\, p$ so $n^{(p-1)} = 1, mod\, p$ provided n is not a multiple of p

We will now use FLT to evaluate expressions of the form $a^b, mod\, p$ where p is prime. Such expressions can be tricky to evaluate if a is large or b is large. Luckily there are two theorems that can help us.

Theorem

If $a = A, mod\, p$ then $a^n = A^n, mod\, p$ where $n = 1, 2, 3, \ldots$

(this theorem is true whether p is prime or not)

for example $273 = 3, mod\, 5$ so $273^{24} = 3^{24}, mod\, 5$

Proof

See section, Modular Arithmetic

Theorem

If $a = A, mod\, p - 1$ then $n^a = n^A, mod\, p$ where $n = 1, 2, 3, \ldots$ and n is not a multiple of p

(this theorem is only true if p is prime)

for example $387 = 3, mod\, 4$ so $97^{387} = 97^3, mod\, 5$

Proof

We will show that:

$153 = 3, mod\, 6$ so $n^{153} = n^3, mod\, 7$

You can prove the general result in the same way.

$n^6 = 1, mod\, 7$ from FLT where $n = 1, 2, 3, \ldots$ and n is not a multiple of p

So

$n^{153} = n^{(6\times25)+3} = n^{(6\times25)} \times n^3 = (n^6)^{25} \times n^3 = 1^{25} \times n^3 = 1 \times n^3 = n^3, mod\, 7$

Example

Evaluate $2518^{10}, mod\, 17$

Now:

$2518 = 2, mod\, 17$ so $2518^{10} = 2^{10}, mod\, 17$

And:

$2^{10} = 1024 = 4, mod\, 17$

Example

Evaluate $3^{220}, mod\, 19$

Now:

$220 = 4, mod\, 18$ so $3^{220} = 3^4, mod\, 19$

And:

$3^4 = 81 = 5, mod\, 19$

Example

Evaluate $875^{302}, mod\, 13$

Now:

$875 = 4, mod\, 13$ so $875^{302} = 4^{302}$

Now:

$302 = 2, mod\, 12$ so $4^{302} = 4^2, mod\, 13$

And:

$4^2 = 16 = 3, mod\, 13$

We will now use FLT to find the last digit of numbers of the form a^b

Note:

If $N = 32748$ then $N = 32740 + 8 = (3274 \times 10) + 8$ so $N = 8, mod\, 10$

Finding the last digit of N is the same as finding $N, mod\, 10$

Note:

If $N=7,mod\,10$ then $N=10k+7$ for some positive integer k

So:

$N=2(5k+3)+1$ so $N=1,mod\,2$

And:

$N=5(2k+1)+2$ so $N=2,mod\,5$

We can repeat these calculations for $N=1,2,3,4,5,6,8,9,mod\,10$ to get this table.

$N,mod\,10$	0	1	2	3	4	5	6	7	8	9
$N,mod\,2$	0	1	0	1	0	1	0	1	0	1
$N,mod\,5$	0	1	2	3	4	0	1	2	3	4

So if we know $N,mod\,2$ and $N,mod\,5$ we can find $N,mod\,10$

for example, if $N=0,mod\,2$ and $N=3,mod\,5$ then $N=8,mod\,10$

Example

Find the last digit of 13^{270}

mod 2

13^{270} is odd so $13^{270}=1,mod\,2$

mod 5

a) $13=3,mod\,5$ so $13^{270}=3^{270},mod\,5$

b) $270=2,mod\,4$ so $3^{270}=3^2=9=4,mod\,5$

iii) Now $13^{270}=1,mod\,2$ and $13^{270}=4,mod\,5$ so from the table $13^{270}=9,mod\,10$

So the last digit of 13^{270} is 9

In 1640, Fermat announced FLT. In1978, Rivest, Shamir and Adleman announced the RSA encryption system. RSA encryption relies on FLT. It has many applications. For example, if enables us to buy stuff online.

See chapter: Encryption

see Exercise

Another proof of FLT

Show that

$(a+b)^7-(a^7+b^7)$ is a multiple of 7

Show that

$(a+b+c)^7-(a^7+b^7+c^7)$ is a multiple of 7

Show that

$(a+b+c+d+...)^7-(a^7+b^7+c^7+d^7+...)$ is a multiple of 7

If there are n numbers $a,b,c,d\ldots$ and we set them all equal to 1 then

n^7-n is a multiple of 7

etc

Yet another proof of FLT

Take any number from $1,2,3,4,5,6$ and write down its first six multiples

for example, take the number 3

$1\times3=3, mod 7$ $\quad 2\times3=6, mod 7$ $\quad 3\times3=2, mod 7$

$4\times3=5, mod 7$ $\quad 5\times3=1, mod 7$ $\quad 6\times3=4, mod 7$

These multiples are just $1,2,3,4,5,6$ in a different order.

Hint: If $n\times3=m\times3$ then $n=m$ Why?

So $(1\times3)\times(2\times3)\times(3\times3)\times(4\times3)\times(5\times3)\times(6\times3)=1\times2\times3\times4\times5\times6$

So $1\times2\times3\times4\times5\times6\times3^6=1\times2\times3\times4\times5\times6$

$3^6=1, mod 7$

etc

EXERCISE

1) Show that:

n^5-n is a multiple of 10 for $n=1,2,3,\ldots$

2) Find:

$7465^5, mod 7$

3) Find:

$18^{163}, mod 41$

4) Find the last digit of:

8^{154}

SOLUTIONS

1) 10 is not prime so we cannot use FLT directly, but ...

$n^5 - n$ is a multiple of 5 by FLT

If n is even then $n^5 - n$ is a multiple of 2

If n is odd then $n^5 - n$ is a multiple of 2

Either way $n^5 - n$ is a multiple of 2 and a multiple of 5 and hence a multiple of 10.

2) $7465 = 3, mod\,7$ so $7465^5 = 3^5 = 243 = 5, mod\,7$

3) $163 = 3, mod\,40$ so $18^{163} = 18^3 = 5832 = 10, mod\,41$

4)

i) mod 2

a) 8^{154} is even so $8^{154} = 0, mod\,2$

ii) mod 5

a) $8 = 3, mod\,5$ so $8^{154} = 3^{154}, mod\,5$

b) $154 = 2, mod\,4$ so $3^{154} = 3^2 = 9 = 4, mod\,5$

iii) from the table

$8^{154} = 4, mod\,10$ so the last digit of 8^{154} is 4

Card Shuffles

I put a pack of eight cards on the table. The top card has an A written on it. The next card has a B written on it, etc

I pick up the top half of the pack, A, B, C, D in my right hand.

I pick up the bottom half of the pack, E, F, G, H in my left hand.

Then I do a riffle shuffle:

I drop the D card from my right hand onto the table, then the H card from my left hand, then the C card from my right hand, then the G card from my left hand, then the B card from my right hand, then the F card from my left hand, then the A card from my right hand, then the E card from my left hand.

The cards are now in the order E, A, F, B, G, C, H, D with the E on the top of the pile. Try it.

Then I shuffle again and again until the cards are back in their original order.

So how have the cards moved?

Order at start	A	B	C	D	E	F	G	H
Order after one shuffle	E	A	F	B	G	C	H	D
Order after two shuffles	G	E	C	A	H	F	D	B
Order after three shuffles	H	G	F	E	D	C	B	A
Order after four shuffles	D	H	C	G	B	F	A	E
Order after five shuffles	B	D	F	H	A	C	E	G
Order after six shuffles	A	B	C	D	E	F	G	H

So the cards are back in their original order after six shuffles.

It will be helpful to look at the position of each card in the pack. Position 1 is the top card etc

Card	A	B	C	D	E	F	G	H
Position at start	1	2	3	4	5	6	7	8
Position after one shuffle	2	4	6	8	1	3	5	7
Position after two shuffles	4	8	3	7	2	6	1	5
Position after three shuffles	8	7	6	5	4	3	2	1
Position after four shuffles	7	5	3	1	8	6	4	2
Position after five shuffles	5	1	6	2	7	3	8	4
Position after six shuffles	1	2	3	4	5	6	7	8

You can check that:

After 1 shuffle, the card starting in position m will end up in position $2m, mod\,9$

After 2 shuffles, the card starting in position m will end up in position $(2\times2)m, mod\,9$

After 3 shuffles, the card starting in position m will end up in position $(2\times2\times2)m, mod\,9$

...

After k shuffles, the card starting in position m will end up in position $2^k m, mod\,9$

If $2^k m=m, mod\,9$ for $m=1,2,...8$ then after k shuffles, the card starting in position m will end up in position m So the cards are back in their original order.

Now $2^6=1, mod\,9$ You can check this.

So $2^6\times1=1, mod\,9$ and $2^6\times2=2, mod\,9$ and $2^6\times3=3, mod\,9$ and $\ldots$ $2^6\times8=8, mod\,9$

So the pack of 8 cards will be back in their original order after 6 shuffles.

In general:

Take a pack of N cards:

If $2^k=1, mod(N+1)$ then the cards will be back in their original order after k shuffles.

We know from Fermat’s little theorem that:

$2^{(p-1)}=1, mod\,p$ provided $p\neq2$

So:

Take a pack of $p-1$ cards: where p is a prime number

Now $2^{(p-1)}=1, mod\,p$ so the cards will be back in their original order after p shuffles.

A pack of 52 cards will be back in its original order after 52 shuffles, because 53 is prime.

Casting-out Nines

Now:

$$8263=(8\times1000)+(2\times100)+(6\times10)+(3)$$

So:

$$8263=(8\times999)+(2\times99)+(6\times9)+(8+2+6+3)$$

So:

$$8263=(9\times\ldots)+(8+2+6+3)$$

So:

$$8263=8+2+6+3\,,mod\,9$$

So to find $N\,,mod\,9$ we just add up the digits of N

If you do an addition, subtraction or multiplication then the answer must be correct in mod 9.

Example 1

Eric says $123+35=157$

mod 9:

$$LHS=123+35=(1+2+3)+(3+5)=6+8+14=5$$

$$RHS=157=1+5+7=13=4$$

end of mod 9

So Eric’s answer must be incorrect.

Example 2

Eric says $3647\times7298=26615797$

mod 9:

$$LHS=3647\times7298=(3+6+4+7)\times(7+2+9+8)=20\times26=2\times8=16=7$$

$$RHS=26615797=2+6+6+1+5+7+9+7=43=7$$

end of mod 9

Be careful. We have not shown that Eric’s answer must be correct.

We have shown that Eric’s answer is either correct or out by a multiple of 9

Perfect Numbers

Example 1

The factors of 28 are:

1, 2, 4, 7, 14 Note: we have included 1 as a factor but not 28

The sum of the factors of 28 is:

$$1+2+4+7+14=28$$

So 28 equals the sum of its factors. So 28 is a perfect number.

Example 2

The factors of $(2^6 p)$ where p is an odd prime, are:

1	2	2^2	2^3	2^4	2^5	2^6
p	$2p$	$2^2 p$	$2^3 p$	$2^4 p$	$2^5 p$	

The sum of the factors of $(2^6 p)$ is:

$$(1+2+2^2+2^3+2^4+2^5+2^6)+p(1+2+2^2+2^3+2^4+2^5)$$

but:

$(1+2+2^2+2^3+2^4+2^5+2^6)=2^7-1$ a geometric series

and:

$(1+2+2^2+2^3+2^4+2^5)=2^6-1$ a geometric series

So the sum of the factors of $(2^6 p)$ is:

$$(2^7-1)+p(2^6-1)$$

If:

$$p=2^7-1$$

then:

the sum of the factors of $(2^6 p)$ is:

$$(2^7-1)+(2^7-1)(2^6-1)=(2^7-1)(1+(2^6-1))=(2^7-1)2^6=2^6 p$$

So $(2^6 p)$ is a perfect number.

Euclid’s theorem:

If 2^k-1 is prime then $2^{k-1}(2^k-1)$ is an even perfect number.

for example:

2^5-1 is prime so $2^4(2^5-1)$ is an even perfect number.

Euler’s theorem:

All even perfect numbers are of the form $2^{k-1}(2^k-1)$ where 2^k-1 is prime

This is much more difficult to prove.

Theorem

All even perfect numbers are triangle numbers

Proof

$$2^{k-1}(2^k-1)=2^k2^{-1}(2^k-1)=\frac{1}{2}(2^k-1)(2^k)$$ which is of the form $\frac{1}{2}n(n+1)$

A conjecture about even perfect numbers:

there are an infinite number of even perfect numbers

Theorem

No odd perfect number is prime

Proof

If p is prime then its only factor is: 1

If p is perfect then $1=p$ and this can’t happen

Theorem

No odd perfect number is a square

Proof

Factors come in pairs (except for 1)

The factors of 24 are:

1 2 and 12 3 and 8 4 and 6

So every integer has an odd number of factors. No!

The factors of 36 are:

1 2 and 18 3 and 12 4 and 96 6

36 has an even number of factors because 36 is a square

So all squares have an even number of factors and all other integers have an odd number of factors.

225 is an odd square

225 has an even number of factors:

1 3 and 75 5 and 45 9 and 25 15

All the factors of 225 are odd. So the sum of the factors of 225 is even.

So 225 is odd but the sum of its factors is even. So 225 cannot be perfect.

All this applies to any odd square. So no odd square is perfect.

A conjecture about odd perfect numbers:

odd perfect numbers do not exist

Amicable pairs

The factors of 220 are:

$1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110$

and:

$1+2+4+5+10+11+20+22+44+55+110=284$

The factors of 284 are:

$1, 2, 4, 71, 142$

and

$1+2+4+71+142=220$

We say 220 and 284 are an amicable pair.

Pythagoras(?) discovered the amicable pair: 220 and 284

Fermat discovered the amicable pair: 17296 and 18416

Descartes discovered the amicable pair: 9363584 and 9437056

Euler then discovered another sixty amicable pairs!

They all missed the pair, 1184 and 1210 which was not discovered until 1866 (by a 16 year old)

Sums of Squares

Some integers are the sum of two squares, for example:

$58=3^2+7^2$ and $64=0^2+8^2$

Some integers are not the sum of two squares, for example:

7 and 15

We want to know which integers are the sum of two squares and which are not.

Theorem

If m and n are both the sum of two squares then mn is the sum of two squares.

Proof

$m=a^2+b^2$ and $n^2=c^2+d^2$

$mn=\ldots=(ac+bd)^2+(ad-bc)^2$

This also means that if m is the sum of two squares then any positive power of m is the sum of two squares.

Theorem

2 is the sum of two squares

Proof

$2=1^2+1^2$

Theorem

No integer of the form $4k+3$ is the sum of two squares

Proof

mod 4:

$x=0,1,2,3$ so $x^2=0,1$ and $y=0,1,2,3$ so $y^2=0,1$

so $x^2+y^2=0,1,2$ so $x^2+y^2\neq 3$

end of mod 4

So an integer of the form $4k+3$ cannot be the sum of two squares.

All primes (except 2) are of the form $4k+1$ or $4k+3$

We have just proved that no prime of the form $4k+3$ is the sum of two squares.

Fermat proved that every prime of the form $4k+1$ is the sum of two squares.

Theorem

Every even power of an integer is the sum of two squares

Proof

$6^{10}=(6^5)^2+0^2$ etc

We can write any integer n in the form:

$n=(2^a)(3^b)(5^c)(7^d)(11^e)(...)$

2 is the sum of two squares

So $(2)^a$ is the sum of two squares.

$5,13,17,...$ are all of the form $4k+1$

So $5,13,17,...$ are all the sum of two squares.

So $(5)^c,(13)^f,(17)^g,...$ are all the sum of two squares.

$3,7,11,...$ are all of the form $4k+3$

So $3,7,11,...$ are not the sum of two squares.

But $(3)^b,(7)^d,(11)^e,...$ are all the sum of two squares if $b,d,e,...$ are all even.

So n is the sum of two squares if all the powers of all the $4k+3$ primes are even.

So $(2^5)(3^{10})(5^{14})(7^2)(11^{24})(13^3)(17^1)$ is the sum of two squares

It turns out that:

n is the sum of two squares if and only if all the powers of all the $4k+3$ primes are even.

So $(2^1)(3^4)(5^0)(7^3)(11^0)(13^0)(17^8)(19^{20})$ is not the sum of two squares

Difference of two squares

Theorem

No integer of the form $4k+2$ is the difference of two squares.

Proof

mod 4:

$x=0,1,2,3$ so $x^2=0,1$ and $y=0,1,2,3$ so $y^2=0,1$

so $x^2 - y^2 = 0, 1, -1$ so $x^2 - y^2 = 0, 1, 3$ so $x^2 - y^2 \neq 2$

end of mod 4

So an integer of the form $4k+2$ cannot be the difference of two squares.

We can easily verify that:

Theorem

Every integer of the form 4k is the difference of two squares

Proof

$$4k = (k+1)^2 - (k-1)^2$$

Also

$$4k+1 = (2k+1)^2 - (2k)^2$$

And

$$4k+3 = (2k+2)^2 - (2k+1)^2$$

So n is the difference of two squares if and only if n is not of the form $4k+2$

see Exercise

Theorem

Every odd prime can be written as the difference of two squares in just one way.

Proof

If:

$$p = n^2 - m^2 = (n-m)(n+m)$$

then:

p can be factorised and is therefore not a prime unless $(n-m)=1$ and $p=(n+m)$

Which means we must have:

$$n = \frac{p+1}{2} \quad \text{and} \quad m = \frac{p-1}{2}$$

It can be proved that:

Every integer is the sum of:

4 squares

9 cubes

19 fourth powers

37 fifth powers

etc

EXERCISE

Show that no integer of the form $8k+7$ is the sum of three squares.

SOLUTION

mod 8

$x=0,1,2,3,4,5,6,7$ so $x^2=0,1,4$

$y=0,1,2,3,4,5,6,7$ so $y^2=0,1,4$

$z=0,1,2,3,4,5,6,7$ so $z^2=0,1,4$

So $x^2+y^2+z^2=0,1,2,3,4,5,6$

end of mod 8