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:

$n = \textit{last digit of } n$

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