Numbers

Mathematics, rightly viewed, possesses not only truth, but supreme beauty.

Bertrand Russell

'Here lies Diophantus,' the wonder behold.
Through art algebraic, the stone tells how old:
'God gave him his boyhood one-sixth of his life,
One twelfth more as youth while whiskers grew rife;
And then yet one-seventh ere marriage begun;
In five years there came a bouncing new son.
Alas, the dear child of master and sage
After attaining half the measure of his father's life chill fate took him.
After consoling his fate by the science of numbers for four years, he ended his life.'

Epitaph of Diophantus (apocryphal)

©2011-14 McQuain

Basic Definitions

Number theory is the branch of mathematics that is concerned (primarily) with the study of the properties of integers.

We'll take the notion of an *integer* as a primitive (undefined) concept we all understand.

A *prime integer* is an integer that is larger than 1 and has no positive *divisors* except itself and 1.

 ©2011-14 McQuain

Divisibility

Suppose that x and y are integers. Then we say that x *divides* y if there exists an integer k such that $y = x * k$.

If x divides y, we write $x \mid y$.

Examples:

13 | 689 because 689 = 13 * 53

9 | 11322 because 11322 = 9 * 1258

To indicate that x does not divide y we put a slash through the |; but it seems that neither MS nor MathType support that symbol.

 ©2011-14 McQuain

More Basic Definitions

We say two integers *x* and *y* are *relatively prime* if 1 is the largest integer that divides both *x* and *y*.

So, 24 and 25 are relatively prime but 24 and 36 are not.

The greatest common divisor or GCD of two integers x and y is the largest integer d such that d | x and d | y.

GCD(12, 16) = 4
GCD(24, 36) = 12
GCD(125, 128) = 1 (so they're relatively prime)

©2011-14 McQuain

Some Theorems

Theorem 1: If $x \mid y$ and $x \mid z$ then for all integers m and n, $x \mid (m*y + n*z)$.

Corollary: If $x \mid y$ then $x \mid y^2$.

Theorem 2: If $x \mid y$ and $y \mid z$ then $x \mid z$.

Theorem 3: If $x \mid y$ and $y \mid x$ then $x = y$ or $x = -y$.

©2011-14 McQuain

Parity as a Heuristic

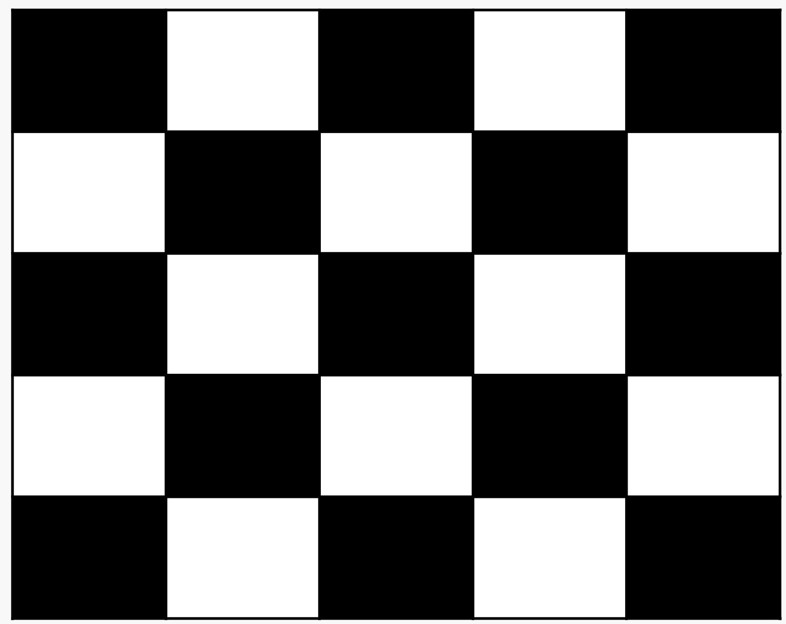
We say an integer is even if it is divisible by 2 and odd if it is not divisible by 2.

This is often referred to as the *parity* of the integer.

The idea is often generalized to situations in which a thing has two possible values, or values of two possible types.

A chess knight makes an L-shaped move, two squares followed by one square, where the first part can be in any vertical or horizontal direction (but never diagonal).

Is it possible to start with a knight in the upper-left square of this mutilated chessboard and jump it around until every square has been visited exactly once and the knight winds up in the original square?



©2011-14 McQuain

Party Guests

Dwight always has a group of friends over to watch the Super Bowl on his 84" 3D plasma TV. In preparation, he buys 84 bottles of beer, knowing that each of his guests always drinks the same number of beers as all the other guests, and that they will drink every bottle of beer that is available. Dwight himself does not drink beer.

How many guests might Dwight invite to his Super Bowl party?

©2011-14 McQuain

Fundamental Theorem of Arithmetic

Every integer *N*, larger than 1, can be expressed uniquely (disregarding order) as a product of primes.

Examples:

36	= 2 * 2 * 3 * 3	= 2^2*3^2
2104	= 2 * 2 * 2 * 263	= 2^3*263
72270	= 2*3*3*5*11*73	= 2*3^2*5*11*73

©2011-14 McQuain

Party Guests Again

Dwight always has a group of friends over to watch the Super Bowl on his 84" 3D plasma TV. In preparation, he buys 84 bottles of beer, knowing that each of his guests always drinks the same number of beers as all the other guests. Dwight himself does not drink beer.

How many guests might Dwight invite to his Super Bowl party?

Now: 84 = 2 * 2 * 3 * 7

So the possible products to form 84 would be:

1 * 84	2 * 42	4 * 21
6 * 14	12 * 7	28 * 3

Each different pair implies two possibilities.

©2011-14 McQuain

A Decanting Problem

You need to have a container holding exactly 1 gallon of water.

You have two jugs, capable of holding 3 and 5 gallons of water, respectively. Unfortunately, neither jug is marked in any way that would allow you to measure how much water was in it if it was partially filled.

You are also near a stream of clear, cold water, so at least you have an effectively infinite supply of that…

Is it possible for you to use your two jugs in such a way that on of them will contain exactly 1 gallon of water and the other jug is empty? If yes, how? If no, why not?

©2011-14 McQuain

Some Analysis

First of all, if we ever reach a state when both jugs are partially filled, we won't be able to determine how much water is in either one… we'll just have to empty them or top them off.

So, it makes no sense to pour water from one jug into the other jug, unless that leaves one jug full or one jug empty.

By the same reasoning, it makes no sense to partially fill either jug from the stream.

And, it makes no sense to pour all the contents of a partially filled jug back into the stream, since that either leaves us with both jugs empty (back to our starting state) or with one jug empty and the other full (which can be reached in one step from our starting state).

So at each step the only reasonable moves are to:

- completely fill an empty jug from the stream
- completely empty a full jug into the stream
- pour from one jug into the other, completely filling or completely emptying one jug and leaving the other jug partially filled

©2011-14 McQuain

Some Algebra

Let x be the total number of times the 3-gallon jug has been filled from the stream or emptied into the stream, but we'll count filling it once as +1 and emptying it once as -1.

Note that 3x then represents the total amount of water that has transferred between the stream and the 3-gallon jug (counting flow into the jug as positive and flow out of the jug as negative).

Let y be the total number of times the 5-gallon jug has been filled from the stream or emptied into the stream, with the same logic as above.

We won't use x or y to measure transfers between the two jugs.

Now, $3x + 5y$ equals the total amount of water that has been removed from the stream.

So, we want to find values of x and y such that

$$3x + 5y = 1,$$

BUT the values of x and y must be integers!

©2011-14 McQuain

Diophantine Equations

A *Diophantine equation* is an equation in which all coefficients are integers and in which we are interested only in integer solutions.

Diophantine equations have a long and storied history in the development of mathematics, going back (at least) to Diophantus of Alexandria (c. 275 CE).

The topic is far too broad to consider in depth here, but we can discuss a few useful techniques.

Currently, we're interested in the *linear* Diophantine equation $3x + 5y = 1$.

 ©2011-14 McQuain

Decanting Again

The linear Diophantine equation 3x + 5y = 1 can be solved easily by trial-and-error techniques, but

- That's only because it has "nice" coefficients, and
- it's no fun to find a solution by trial-and-error anyway.

For linear Diophantine equations of the form ax + by = c, where c is the greatest common divisor of a and b, there is simple tabular solution method:

	x	y	d	k
	1	0	3	
	0	1	5	0 ← 3/5, remainder = 3
2-up – k*1-up →	1	0	3	1 ← 5/3, remainder = 2
	-1	1	2	1 ← 3/2, remainder = 1
	2	-1	1	2 ← 2/1, remainder = 0 so stop

This yields the solution 3 * 2 + 5 * -1 = 1, but what does this mean?

©2011-14 McQuain

Decanting Solution

Our linear Diophantine equation for the decanting problem, $3x + 5y = 1$ has the solution $x = 2$, $y = -1$.

But what does that mean? I.e., how do we obtain 1 gallon?

Well, the simplest interpretation is that it indicates we fill the 3-gallon jug from the stream 2 times and we empty the 5-gallon jug into the stream once.

Clearly then, we start by filling the 3-gallon jug from the stream:	3	0
Now all we can do next is pour the 3-gallon jug into the other one:	0	3
Now, all we can do is fill the 3-gallon jug again:	3	3
Now, all we can do is pour from the 3-gallon jug into the other one:	1	5
Finally then, empty the 5-gallon jug into the stream:	1	0

Aha!

©2011-14 McQuain

Another Theorem

Theorem 4: If the linear Diophantine equation Ax + By = C is such that A and B are relatively prime, then:

a) There are integers x_0 and y_0 that satisfy the equation.

b) Every pair of integers given by the following formulas also satisfy the equation:

$$x = x_0 + Bk \qquad y = y_0 - Ak$$

where k is an arbitrary integer.

So, since the linear Diophantine equation 3x + 5y = 1 is satisfied by $x_0 = 2$, $y_0 = -1$, then we also have the following solutions:

$$x = 2 + 5k \qquad y = -1 - 3k$$

So another solution would be x = 7 and y = -4… can you interpret that?

©2011-14 McQuain

Another Decanting Problem

You need to have a container holding exactly 1 gallon of water.

You have two jugs, capable of holding 4 and 6 gallons of water, respectively. Unfortunately, neither jug is marked in any way that would allow you to measure how much water was in it if it was partially filled.

You are also near a stream of clear, cold water, so at least you have an effectively infinite supply of that…

Is it possible for you to use your two jugs in such a way that one of them will contain exactly 1 gallon of water? If yes, how? If no, why not?

©2011-14 McQuain

Solution

In this case, we would have the following linear Diophantine equation:

$$4x + 6y = 1$$

Now, $2 \mid 4$ and $2 \mid 6$, so by Theorem 1 it must be true that $2 \mid 4x + 6y$ for all possible integer values of x and y.

So, if this Diophantine equation has a solution, we would have that $2 \mid 1$, which is clearly false. Therefore, the equation must have no solutions.

©2011-14 McQuain

Animal Auction

Henry, Eli, Cornelius and their wives Gertrude, Katherine, and Anna (not necessarily in that order) each purchased at least one animal at a farm auction. No two of them purchased the same number of animals.

The price (in dollars) that each of them paid for each animal was equal to the number of animals that he or she bought.

Henry purchased 23 more animals than Katherine did, and Eli spent $11 more per animal than Gertrude did. Also, each husband spent a total of $63 more than his wife.

Who was married to whom?

©2011-14 McQuain

Confused Teller

It was a strange lapse on the part of the bank teller. Evidently, he misread the check, for he handed out the amount of dollars in cents and the amount of cents in dollars.

When the mistake was pointed out to him, he became flustered, made an absurd mathematical error, and handed out one dollar, one dime and one cent more.

But the depositor declared that he was still short of the correct amount of money.

The teller finally pulled himself together, doubled the amount he had already given to the depositor (that is, he handed the depositor an additional amount equal to the total amount he had given the depositor previously), and that settled the transaction to everyone's satisfaction.

What was the amount of the check?

©2011-14 McQuain

Floor and Ceiling

Let x be a real number.

The ceiling of x, written ceil(x) or $\lceil x \rceil$, is the smallest integer N such that $N \geq x$.

The floor of x, written floor(x) or $\lfloor x \rfloor$, is the largest integer N such that $N \leq x$.

If x is a real number, then $x = \lfloor x \rfloor + \alpha$ where $0 \leq \alpha < 1$.

If x is a real number, then $x = \lceil x \rceil + \beta$ where $-1 < \beta \leq 0$.

©2011-14 McQuain

Some Theorems: Floor and Ceiling

If x and y are a real numbers and k is an integer, then:

$\lfloor x \rfloor = k$ if and only if $k \le x < k+1$

$\lceil x \rceil = k$ if and only if $k-1 < x \le k$

$\lfloor x+k \rfloor = \lfloor x \rfloor + k$

$\lceil x+k \rceil = \lceil x \rceil + k$

$\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x+y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$

$\lceil x \rceil + \lceil y \rceil - 1 \le \lceil x+y \rceil \le \lceil x \rceil + \lceil y \rceil$

©2011-14 McQuain

Aside: Proofs

If x is a real number and k is an integer, then: $\lfloor x+k \rfloor = \lfloor x \rfloor + k$

proof :

Let x be a real number and k be an integer. Then $x + k = \lfloor x+k \rfloor + \alpha$, where $0 \le \alpha < 1$.

So, $\lfloor x+k \rfloor = (x-\alpha) + k$, and since $x-\alpha$ is an integer and $0 \le \alpha < 1$, $x-\alpha$ must equal $\lfloor x \rfloor$. Therefore, $\lfloor x+k \rfloor = \lfloor x \rfloor + k$.

©2011-14 McQuain

Some Theorems: Prime Numbers

Let p be a prime number, and m and n be integers.

If $p \mid mn$ then $p \mid m$ or $p \mid n$.

If k is a positive integer, and $p^k \mid m$ then $p \mid m$.

©2011-14 McQuain

Quotient/Remainder Theorem

Let x and d be integers, $d \neq 0$.

Then there exist unique integers q and r such that

$$x = qd + r$$

and

$$0 \leq r < d.$$

Example:

```
        1874
    +-------
39  | 73094
      39
      ---
      340
      312
      ----
       289
       273
       ----
        164
        156
        ---
          8
```

quotient

divisor

dividend

remainder

We write: $x \bmod N$ for the remainder when x is divided by N.

©2011-14 McQuain

Congruence Modulo N

Let x, y, and N be integers, $N \neq 0$.

We say that x *is congruent to* y *modulo* N iff $N \mid (x - y)$.

We write this as $x \equiv y \bmod N$.

Observation: $x \equiv y \bmod N$ iff $x \bmod N = y \bmod N$.

 ©2011-14 McQuain

Congruence Facts

Reflexivity: $x \equiv x \bmod N$

Symmetry: $x \equiv y \bmod N$ iff $y \equiv x \bmod N$

Transitivity: if $x \equiv y \bmod N$ and $y \equiv z \bmod N$ then $x \equiv z \bmod N$

Fermat's Little Theorem

If p is prime and a is an integer, then $a^p \equiv a \bmod p$.

©2011-14 McQuain

Diophantine Equations Again

Suppose we want to solve the Diophantine equation: $66x + 48y = 30$.

We can simplify the problem by dividing through by the GCD of the three coefficients:

$$11x + 8y = 5$$

Now, the equation is satisfied iff:

$$(11x + 8y) \bmod 8 = 5 \bmod 8$$

But, $8y \bmod 8 = 0$, so the equation is satisfied iff:

$$11x \bmod 8 = 5 \bmod 8 \text{ or in other words } 11x \equiv 5 \bmod 8.$$

So, we need to find an integer M that's a multiple of 11 and congruent to 5 mod 8.

Start with the smallest positive value congruent to 5 mod 8 and work your way up:

5, 13, 21, 29, 37, 45, 53, 61, 69, 77

So, $11x = 77$ or $x = 7$ will work. And from the second equation, we see that $y = -9$.

©2011-14 McQuain

Another Problem

The annual dues for the Burbank Book Club are usually $23 per person. However, senior citizens pay only $17.

This year the Club collected a total of $1500 was collected in dues.

What is the smallest number of senior citizens that could be members of the Club?

©2011-14 McQuain

Another Problem

A census taker stopped at the Princeton Hilton, and asked how many guests were currently at the hotel.

Dwight, the clerk at the desk was a mathematics major at the local college, and had a questionable sense of humor. He replied that the number of guests was the smallest positive integer that had the following two properties:

- when divided by 2, the result is a perfect square
- when divided by 3, the result is a perfect cube

The census taker, who had been calculating all day, slammed his notebook on the hotel desk, screamed "I quit!", and stormed out.

How many guests were staying at the hotel that day?

©2011-14 McQuain