TOURNAMENT OF THE TOWNS, 2003–2004

$\mathbb{N}$umber Theory Notes

Number Theory is mainly concerned with properties of the *natural numbers* (or *positive integers*) $\mathbb{N} = \mathbb{Z}^+ = \{1, 2, 3, \dots\}$ and the *integers* $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.

Divisibility If $a, b \in \mathbb{Z}$ we say: *a divides b*, and write: $a \mid b$, if $b = aq$ for some integer q. Otherwise, *a does not divide b* and we write: $a \nmid b$.

If $a \mid b$ then we also say: a is a *divisor* (or *factor*) of b, or that: b is a *multiple* of a.

Property 1. *If $a \mid b$ and $a \mid c$ then $a \mid bx + cy$ for any integers x, y.*

Divisibility rules For any integer n,

$2 \mid n$ if 2 divides the last digit of n
$3 \mid n$ if 3 divides the *sum* of the digits of n
$4 \mid n$ if 4 divides the number formed by the last 2 digits of n
$5 \mid n$ if 5 divides the last digit of n, i.e. n ends in 0 or 5
$6 \mid n$ if 2 divides n *and* 3 divides n
$8 \mid n$ if 2 divides the number formed by the last 3 digits of n
$9 \mid n$ if 9 divides the *sum* of the digits of n
$10 \mid n$ if the last digit of n is 0
$11 \mid n$ if 11 divides the difference of the sums of the odd-placed digits and the even-placed digits
$12 \mid n$ if 3 divides n *and* 4 divides n

Prime numbers A *prime number* is a *natural number* larger than 1 that is only divisible by *itself* and 1. A *natural number* that is neither 1 nor prime is called *composite*. The number 1 is neither *prime* nor *composite*; in fact, it is a *unit* (the technical term for a number that divides all integers).

Fundamental theorem of arithmetic. *Any natural number n, other than 1, can be written* uniquely *as a product of primes.*

e.g. $74844 = 2^2.3^5.7.11$. Such a factorisation is called a *prime decomposition*. (Note that if we were to include 1 as a prime then $74844 = 1^5.2^2.3^5.7.11$, say, would be “another prime decomposition”. Excluding 1 as a prime ensures the *uniqueness* of *prime decompositions*.)

Euclid’s Lemma. *If a prime p divides ab then $p \mid a$ or $p \mid b$.*

Greatest common divisor The *greatest common divisor* (or *highest common factor*) of two integers a, b, denoted by $\gcd(a, b)$ or $\mathrm{hcf}(a, b)$ or simply (a, b), is the largest natural number that divides both a and b. (Here we must insist that a and b are not both zero.)

Relatively prime If $(a, b) = 1$ then a, b are said to be *relatively prime* or *coprime.*

Division Algorithm. *For integers* a, b *with* $a \neq 0$ *there exist integers* q *(the quotient) and* r *(the remainder) such that*

$$b = aq + r \text{ and } 0 \leq r < a.$$

Essentially q, r *are the numbers that make the following division work:*

$$\begin{array}{l} \quad q \;\; \textit{rem.} \;\; r \\ a\,\overline{)\,b \qquad\qquad} \end{array}$$

Greatest common divisor properties If d is the gcd of two integers a, b then

- d also divides $a - bm$ for any integer m;
- $d = (a - bm, b)$ for any integer m;
- there are integers x, y such that $d = ax + by$.

Euclidean algorithm The *Euclidean algorithm* is an efficient method of finding the gcd d of two integers a, b and also (by retracing the steps of the algorithm) two integers x, y such that $d = ax + by$. It is best explained via an example (see below).

Example 1. *To find the* gcd *of 234 and 180, perform the following steps.*

1. *Draw 3 parallel vertical lines.*
2. *Write 234 and 180 in the two internal columns.*
3. *Divide the* smaller *number 180 into the* larger *234. Write the* quotient *in the column adjacent to 234, and the* remainder *below 234.*
4. *Repeatedly divide back and forth in a similar way to* Step 3. *until one number* divides *(*evenly*) into the other. At this point that number is the* gcd.

$$\begin{array}{c|r|r|c} & 234 & 180 & \\ 1 & 180 & 162 & 3 \\ \cline{2-3} & 54 & 18 & \end{array}$$

Here 180 was divided into 234, it went once remainder *54; then 54 was divided into 180, it went 3 times* remainder *18; and 18* divides *54 (so we stop) . . . and so 18 is the* gcd *of 234 and 180.*

Working backwards we can also find x, y *such that* $234x + 180y = 18$:

$$\begin{aligned} 18 &= 180 - 162 \\ &= 180 - 3.54 \\ &= 180 - 3(234 - 1.180) \\ &= 4.180 - 3.234. \end{aligned}$$

So $x = 4$ *and* $y = -3$ *is one possibility. All pairs* x, y *satisfy*

$$\begin{aligned} x &= 4 + 13t \\ y &= -3 - 10t \end{aligned}$$

for some integer t.

Linear Diophantine equation An equation of form $ax + by = c$ where x, y are unknown is a *linear Diophantine equation.* For it to have solutions over the integers the gcd d of a, b must divide c.

Least common multiple The *least common multiple* of two integers a, b, denoted by $\mathrm{lcm}(a, b)$, is the least natural number that is a multiple of both a and b. (The *lowest common denominator* of two fractions is the lcm of the denominators of the fractions.)

The following property of the lcm of a, b links it with the gcd of a, b:

$$\text{if } a \text{ and } b \text{ are not both zero then } \mathrm{lcm}(a, b) = \frac{|a.b|}{\gcd(a, b)}.$$

Congruence modulo an integer If two integers a, b have the same remainder on division by a natural number m then "a is *congruent* to b *modulo* m", which is written

$$a \equiv b \pmod{m}$$

Properties of congruence Congruence behaves similarly to $=$, in that for integers a, b, c, d, m,

- if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.
- if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then

$$\begin{aligned} a + c &\equiv b + d \pmod{m} \\ a.c &\equiv b.d \pmod{m} \end{aligned}$$

- if $a \equiv b \pmod{m}$ and n is a natural number then

$$a^n \equiv b^n \pmod{m}.$$

  This follows from the previous (multiplication) property.

Divisibility and Congruence The following statements are equivalent (i.e. mean the same thing), where m is a natural number and b, r are integers.

- m divides b.
- $m \mid b$.
- $b = mq$ for some integer q.
- $b \equiv 0 \pmod{m}$.

- m divides $b - r$.
- $m \mid b - r$.
- $b = mq + r$ for some integer q.
- $b \equiv r \pmod{m}$.

Lemma 1. *If $ac \equiv bc \pmod{m}$ and $(c, m) = 1$ then $a \equiv b \pmod{m}$.*

Lemma 2. *If $ac \equiv bc \pmod{m}$ and $(c, m) = d$ then $a \equiv b \pmod{m/d}$.*

Lemma 3. *If n is an integer and $S(n)$ is the sum of the digits of n then*

$$\begin{aligned} n &\equiv S(n) \pmod 3 \\ \textit{and } n &\equiv S(n) \pmod 9 \end{aligned}$$

Fermat's Little Theorem. *If $n \in \mathbb{N}$, p is a prime and $p \not| n$ then $n^{p-1} \equiv 1 \pmod p$.*

Corollary. *If $n \in \mathbb{N}$, p is a prime then $n^p \equiv n \pmod p$.*