MT1010: Topics in Mathematics: Divisibility of integers

Nik Ruškuc

September 15, 2014

1. Divisibility of Integers

This series of lectures will be concerned with *number theory*. This one of the oldest branches of mathematics (together with geometry), and is concerned with properties of integers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. One important fact about integers is that out of the four basic arithmetical operations of addition, subtraction, multiplication and division, the first three are defined for any pair of integers, whereas the last one is not (e.g. $3/2$). Instead, one can divide with a quotient and remainder:

Basic Fact. *For every two integers a and b with $b > 0$ there exist unique integers q and r such that*

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

q is called the quotient *and r is called the* remainder.

We are going to take this fact for granted. It can be proved starting from the standard Peano axioms for number theory, but this is beyond the scope of the present course. The remarkable fact is that many other well known properties of integers follow from this basic one, as we will see in this course.

Example 1.1. Dividing 17 by 8 gives: $17 = 8 \cdot 2 + 1$. Dividing 20 by 5 gives: $20 = 5 \cdot 4 + 0$.

Definition 1.2. For two integers a and b with $b \neq 0$ we say that b *divides* a or that a *is divisible by* b if $a = bq$ for some q; this is denoted by $b \mid a$.

Here is an easy fact, that is often used in problems:

Theorem 1.3. *The square of an integer is either divisible by* 4*, or else it gives remainder 1 when divided by* 8*.*

Proof. The possible remainders of a when divided by 4 are 0, 1, 2 and 3. In each of these cases we have

$$\begin{array}{lcl} a = 4k & \Rightarrow & a^2 = 16k^2 = 4(4k^2) \\ a = 4k+1 & \Rightarrow & a^2 = (4k+1)^2 = 16k^2 + 8k + 1 = 8(2k^2+1) + 1 \\ a = 4k+2 & \Rightarrow & a^2 = (4k+2)^2 = 16k^2 + 16k + 4 = 4(4k^2+4k+1) \\ a = 4k+3 & \Rightarrow & a^2 = (4k+3)^2 = 16k^2 + 24k + 9 = 8(2k^2+3k+1) + 1. \end{array}$$

■

In the next theorem we give some standard properties of the divisibility relation. They should all be self-evident, although you might want to try and prove a selection.

Theorem 1.4 (Basic properties of $|$) *The following hold for all integers a, b, c, d, x, y:*

(i) $a \mid 0$, $1 \mid a$, $a \mid a$.

(ii) $a \mid 1 \Leftrightarrow a = \pm 1$.

(iii) $a \mid b \;\&\; c \mid d \Rightarrow ac \mid bd$.

(iv) $a \mid b \;\&\; b \mid c \Rightarrow a \mid c$.

(v) $a \mid b \;\&\; b \mid a \Rightarrow a = \pm b$.

(vi) $a \mid b \;\&\; a \mid c \Rightarrow a \mid (bx + cy)$.

Even the way we write out numbers (positional notation) depends on the Basic Fact.

Theorem 1.5 (Positional notation) *Let $b > 1$ be a fixed integer. Every positive integer a can be written as*

$$a = d_{n-1}b^{n-1} + d_{n-2}b^{n-2} + \ldots + d_1 b + d_0$$

where $n \geq 1$ and $0 \leq d_i < b$ for all $i = 0, \ldots, n-1$. Moreover, n and all d_i are uniquely determined.

Proof. We prove the theorem by induction on a. When $a = 1$ (and, more generally, when $a < b$) there is nothing to prove. For $a > 1$, divide a by b:

$$a = qb + d_0, \; 0 \leq d_0 < b.$$

Since $b > 1$, we certainly have $q < a$. By induction, we can write

$$q = d_{n-1}b^{n-2} + d_{n-2}b^{n-3} + \ldots + d_1,$$

with $0 \leq d_i < b$, giving

$$a = d_{n-1}b^{n-1} + d_{n-2}b^{n-2} + \ldots + d_1 b + d_0$$

as required.

Now, for uniqueness, assume that a can also be written as

$$\begin{aligned} a &= f_{m-1}b^{m-1} + f_{m-2}b^{m-2} + \ldots + f_1 b + f_0 \\ &= b(f_{m-1}b^{m-2} + f_{m-2}b^{m-3} + \ldots + f_1) + f_0 \\ &= bq_1 + f_0. \end{aligned}$$

By the Basic Fact we must have $f_0 = d_0$. It then follows that $q_1 = q$, and then, by induction, that $m = n$ and $d_i = f_i$ for all i. ■

Notation 1.6. *In the above theorem, b is called the* base*, and d_i are called the* digits*. We write $a = \overline{(d_{n-1}d_{n-2}\ldots d_1 d_0)}_b$, or when there is no danger of confusion, just $a = d_{n-1}d_{n-2}\ldots d_1 d_0$.*

The above theorem tells us how to find the digits of a number a with respect to a base b:

- Divide a by b: $a = qb + r$;
- r is the last digit;
- Rename: $a := q$;
- Repeat the above steps until $a = 0$.

Example 1.7. Let us express 19 in the base 2 (binary system):

19	1
9	1
4	0
2	0
1	1
0	

Thus $19 = \overline{10011}_2$. Let us now express it in the base 3:

19	1
6	0
2	2
0	

Thus $19 = \overline{201}_3$.

1	3	5	7
9	11	13	15
17	19	21	23
25	27	29	31
33	35	37	39
41	43	45	47
49	51	53	55
57	59	61	63

2	3	6	7
10	11	14	15
18	19	22	23
26	27	30	31
34	35	38	39
42	43	46	47
50	51	54	55
58	59	62	63

4	5	6	7
12	13	14	15
20	21	22	23
28	29	30	31
36	37	38	39
44	45	46	47
52	53	54	55
60	61	62	63

8	9	10	11
12	13	14	15
24	25	26	27
28	29	30	31
40	41	42	43
44	45	46	47
56	57	58	59
60	61	62	63

16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63

32	33	34	35
36	37	38	39
40	41	42	43
44	45	46	47
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63

Figure 1: 'Guessing' a number

Example 1.8. The following trick is based on the idea of positional notation. See if you can figure out why it works. First choose a number between 1 and 63. Let us say that we have chosen 54. Now find in which tables from Figure 1 this number appears. In our case, this is in tables 2, 3, 5 and 6. Add the numbers in the top left corners of these tables: $2 + 4 + 16 + 32 = 54$!

2. Greatest Common Divisor and the Euclidean Algorithm

Definition 2.1. For two integers a and b (at least one of which is not 0), their *greatest common divisor* $\gcd(a, b)$ is the largest positive integer d which divides a and b. In other words, it is the unique number with the following properties:

- $d \mid a$ and $d \mid b$;
- $c \mid a \ \& c \mid b \Rightarrow c \leq d$.

If $\gcd(a, b) = 1$ then a and b are said to be *co-prime*.

Example 2.2. $\gcd(12, 30) = 6$; $\gcd(14, 25) = 1$, so 14 and 25 are co-prime.

Although computing $\gcd(a, b)$ by direct inspection of common divisors is fairly easy for small a and b, it is not so for larger ones. The question of finding a 'cleverer' method then arises naturally. The first step towards such a method is the following

Lemma 2.3. *If a, b, q, r are integers satisfying $a = qb + r$ then* $\gcd(a, b) = \gcd(b, r)$.

Proof. Let $d_1 = \gcd(a, b)$ and $d_2 = \gcd(b, r)$. We have

$$d_1 \mid a \;\&\; d_1 \mid b \Rightarrow d_1 \mid b \;\&\; d_1 \mid r \Rightarrow d_1 \leq d_2$$
$$d_2 \mid b \;\&\; d_2 \mid r \Rightarrow d_2 \mid a \;\&\; b \mid r \Rightarrow d_2 \leq d_1,$$

and so $d_1 = d_2$ as required. ■

If we start with $a > b$, then the above lemma replaces computing of $\gcd(a, b)$ by computing the gcd of two smaller number b and r. Repeating this, gives us the following algorithm for computing $\gcd(a, b)$ $(a > b)$:

Euclidean Algorithm.

- Divide a by b: $a = bq + r$.
- Rename: $a := b$; $b := r$.
- Repeat until $r = 0$.
- The last non-zero remainder is equal to $\gcd(a, b)$.

This algorithm was first described by the famous Greek mathematician Euclid.

Example 2.4. Let us compute $\gcd(231, 133)$ by using the euclidean algorithm:

$$\begin{aligned} 231 &= 1 \cdot 133 + 98 \\ 133 &= 1 \cdot 98 + 35 \\ 98 &= 2 \cdot 35 + 28 \\ 35 &= 1 \cdot 28 + 7 \\ 28 &= 4 \cdot 7 + 0. \end{aligned}$$

Hence $\gcd(231, 133) = 7$.

If we work backwards through the euclidean algorithm, expressing each r in terms of a and b we obtain:

Corollary 2.5. *For any two integers a and b (not both equal to 0) there exist integers α and β such that* $\gcd(a, b) = \alpha a + \beta b$. *($\gcd(a, b)$ is an integer linear combination of a and b.)*

Example 2.6. Working backwards through Example 2.4 we see that

$$\begin{aligned} 7 &= 35 - 28 \\ &= 35 - (98 - 2 \cdot 35) \\ &= 3 \cdot 35 - 98 \\ &= 3 \cdot (133 - 98) - 98 \\ &= 3 \cdot 133 - 4 \cdot 98 \\ &= 3 \cdot 133 - 4 \cdot (231 - 133) \\ &= -4 \cdot 231 + 7 \cdot 133. \end{aligned}$$

In fact, we can do it all at once, as in the following example.

Example 2.7. Let us calculate $\gcd(a, b)$ for $a = 2378$ and $b = 1769$ and express it in the form $\alpha a + \beta b$:

a	$=$	2378				
b	$=$	1769	1769	$=$	b
$a - b$	$=$	609	1218	$=$	$2a - 2b$
$-2a + 3b$	$=$	551	551	$=$	$-2a + 3b$
$3a - 4b$	$=$	58	522	$=$	$27a - 36b$
		58	29	$=$	$-29a + 39b$
		0			

Therefore $\gcd(2378, 1769) = 29 = (-29) \cdot 2378 + 39 \cdot 1769$.

3. The Fundamental Theorem of Arithmetic

Definition 3.1. An integer $p > 1$ is called a *prime* if its only positive divisors are 1 and p.

Example 3.2. The first few primes are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,....

Primes are 'building blocks' of which all the other integers are 'made':

Theorem 3.3 (Fundamental Theorem of Arithmetic) *Every integer $n > 1$ can be written uniquely in the form*

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r},$$

where $p_1 < p_2 < \dots < p_r$ are primes and all k_j are positive integers.

In the proof of the above theorem we will need the following auxiliary results:

Lemma 3.4. *If r, s, t are integers such that* $\gcd(r, s) = 1$ *and* $r \mid st$ *then* $r \mid t$.

Proof. By Corollary 2.5 we have

$$\alpha r + \beta s = 1$$

for some α, β. Also, $r \mid st$ implies that $ru = st$ for some u. Now we have

$$t = t \cdot 1 = t(\alpha r + \beta s) = \alpha rt + \beta st = \alpha rt + \beta ru,$$

and so $r \mid t$. ■

Lemma 3.5. *The following hold for a prime p:*

(i) if $p \mid ab$ then $p \mid a$ or $p \mid b$;

(ii) if $p \mid a_1 a_2 \dots a_s$ then $p \mid a_i$ for some i;

(iii) if $p \mid q_1 q_2 \dots q_t$ and each q_i is a prime, then $p = q_j$ for some j.

Proof. (i) If $p \mid a$ there is nothing to prove. Otherwise we must have $\gcd(p, a) = 1$ (since the only divisors of p are 1 and p) and the statement follows from Lemma 3.4.

(ii) This can be proved by induction on s. If $s = 1$ there is nothing to prove, whereas when $s = 2$ the statement is (i). For $s > 2$ we have $p \mid a_1 a_2 \dots a_{s-1}$ or $p \mid a_s$ by (i). In the latter case we are finished, while in the former by induction we have $p \mid a_i$ for some i.

(iii) This follows from (ii), because each q_i has no divisors other than 1 and q_i. ■

Proof. (of Theorem 3.3) We first prove by induction that n can be written as a product of prime powers. If n is a prime there is nothing to prove. Otherwise $n = st$, where $1 < s, t < n$. By induction both s and t can be written as products of prime powers, and multiplying them together we obtain the required decomposition of n.

To show the uniqueness, we assume that n can be expressed in the required form in two different ways:

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{l_1} q_2^{l_2} \dots q_t^{l_t}. \tag{1}$$

Now, note that

$$p_i \mid n = q_1^{l_1} q_2^{l_2} \dots q_t^{l_t},$$

so that, by Lemma 3.5 (iii), we have $p_i = q_j$ for some j. Similarly, each q_l is equal to some p_m, and so we conclude that

$$r = t,\ p_1 = q_1,\ ldots,\ p_r = q_r.$$

Now (1) becomes

$$p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = p_1^{l_1} p_2^{l_2} \dots p_r^{l_r}.$$

Assume now that for some i we have $k_i \neq l_i$; let us say $k_i > l_i$. Then

$$p_1^{k_1} p_2^{k_2} \dots p_{i-1}^{k_{i-1}} p_i^{k_i - l_i} p_{i+1}^{k_{i+1}} \dots p_r^{k_r} = p_1^{l_1} p_2^{l_2} \dots p_{i-1}^{l_{i-1}} p_{i+1}^{l_{i+1}} \dots p_r^{l_r}.$$

Lemma 3.5 (iii) now gives that p_i is equal to one of $p_1, \dots, p_{i-1}, p_{i+1}, \dots, p_r$, a contradiction. ■

Example 3.6. $180 = 2^2 \cdot 3^2 \cdot 5$.

We can use the decomposition into a product of prime powers to find all the divisors of a given number

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}.$$

Indeed, if $m \mid n$, then decomposing m:

$$m = q_1^{l_1} q_2^{l_2} \dots q_t^{l_t},$$

and using Lemma 3.5 (iii), we see that each q_i is equal to some p_j, and that $l_i \leq k_j$. We conclude that the divisors of n are precisely the numbers of the form

$$p_1^{s_1} p_2^{s_2} \dots p_r^{s_r},$$

where $0 \leq s_i \leq k_i$, $i = 1, \dots, r$.

Example 3.7. The divisors of 180 are

$$\begin{array}{lllllllll}
1 & = & 2^0 \cdot 3^0 \cdot 5^0 & 9 & = & 2^0 \cdot 3^2 \cdot 5^0 & 15 & = & 2^0 \cdot 3^1 \cdot 5^1 \\
2 & = & 2^1 \cdot 3^0 \cdot 5^0 & 18 & = & 2^1 \cdot 3^2 \cdot 5^0 & 30 & = & 2^1 \cdot 3^1 \cdot 5^1 \\
4 & = & 2^2 \cdot 3^0 \cdot 5^0 & 36 & = & 2^2 \cdot 3^2 \cdot 5^0 & 60 & = & 2^2 \cdot 3^1 \cdot 5^1 \\
3 & = & 2^0 \cdot 3^1 \cdot 5^0 & 5 & = & 2^0 \cdot 3^0 \cdot 5^1 & 45 & = & 2^0 \cdot 3^2 \cdot 5^1 \\
6 & = & 2^1 \cdot 3^1 \cdot 5^0 & 10 & = & 2^1 \cdot 3^0 \cdot 5^1 & 90 & = & 2^1 \cdot 3^2 \cdot 5^1 \\
12 & = & 2^2 \cdot 3^2 \cdot 5^0 & 20 & = & 2^2 \cdot 3^0 \cdot 5^1 & 180 & = & 2^2 \cdot 3^2 \cdot 5^1.
\end{array}$$

4. Properties of Primes

Primes have been a subject of study from the ancient times, and many deep theorems have been proved about them. On the other hand, there are many questions, which are very easy to state, but which have not been answered.

We begin with an important fact, known already to Euclid.

Theorem 4.1. *There are infinitely many primes.*

Proof. By way of contradiction, let us assume that $p_1, p_2, \ldots, p_n$ are all the primes. Consider the number

$$P = p_1 p_2 \ldots p_n + 1.$$

It must be divisible by a prime, say p_i. But then

$$p_i \mid P - p_1 p_2 \ldots p_n = 1,$$

a contradiction. ■

One can vary this argument to show that there are infinitely many primes of certain special form. For instance, it is easy to see that every prime number greater than two must have one of the forms $4k+1$ or $4k+3$ (because the numbers of the form $4k$ and $4k+2$ are even).

Theorem 4.2. *There are infinitely many primes of the form* $4k+3$.

Proof. Assume that $p_1, p_2, \ldots, p_n$ are all the primes of the form $4k+3$. Form the number

$$N = 4p_1 p_2 \ldots p_n - 1 = 4(p_1 p_2 \ldots p_n - 1) + 3.$$

Notice that the product of numbers of the form $4k+1$ again has that form:

$$(4k+1)(4l+1) = 4(4kl + k + l) + 1.$$

Therefore, N must have at least one prime divisor, say p_i, of the form $4k+3$. But then

$$p_i \mid 4p_1 p_2 \ldots p_n - N = 1,$$

a contradiction. ■

Similarly, every prime number greater than 3 has the form $6k+1$ or $6k+5$. Indeed a number of the form $6k$ is divisible by 6 (and hence not a prime); a number of the form $6k+2$ or $6k+4$ is even; a number of the form $6k+3$ is divisile by 3. It is possible to modify the above argument to show that there are infinitely many primes of the form $6k+5$. In fact, there are also infinitely many primes of the forms $4k+1$ and $6k+1$, but this is harder to prove. All these results are special cases of the following theorem proved by Dirichlet:

Theorem 4.3. *If a and b are co-prime positive integers then there are infinitely many primes of the form $ak+b$ ($k = 0, 1, 2, \ldots$).*

Note that we do not claim that *every* number of the form, say, $6k+1$ is prime; indeed $6 \cdot 4 + 1 = 25 = 5 \cdot 5$). In fact there is no known simple formula which would give us only prime numbers. For some time mathematicians believed that

$$f(n) = n^2 + n + 41$$

is such a formula, having been checked for $n = 1, 2, \ldots 39$. But, of course,

$$f(40) = 40^2 + 40 + 41 = 40 \cdot 41 + 41 = 41^2$$

is not prime. In fact:

Theorem 4.4. *There is no non-constant polynomial $f(n)$ with integer coefficients which takes on only prime values for all non-negative integers n.*

Proof. Assume that

$$f(n) = a_k n^k + \ldots + a_1 n + a_0$$

is such a polynomial. Then $f(0) = a_0$ is a prime, and so are

$$f(ta_0) = a_k a_0^k t^k + \ldots a_1 a_0 t + a_0$$

for all $t = 1, 2, \ldots$. But clearly $a_0 \mid f(ta_0)$, and, since $f(ta_0)$ is a prime, we must have $f(ta_0) = a_0$ for all $t = 1, 2, \ldots$. So the polynomial $f(n)$ takes the value a_0 infinitely many times, and so it must be the constant polynomial with that value. ■

If we cannot easily generate the prime numbers, it is natural to ask if we can say anything about their distribution among the other numbers. One easy such result is the following:

Theorem 4.5. *If p_n denotes the nth prime then*

$$p_n \leq 2^{2^{n-1}}.$$

Proof. The proof is by induction. Clearly for $n = 1$ we have

$$p_1 = 2 = 2^{2^{1-1}}.$$

The inductive step relies on the proof of Theorem 4.1, which gives

$$\begin{aligned} p_{n+1} &\leq p_1 p_2 \ldots p_n + 1 \\ &\leq 2 \cdot 2^2 \cdot \ldots \cdot 2^{2^{n-1}} + 1 \\ &= 2^{1+2+\ldots 2^{n-1}} + 1 \\ &= 2^{2^n - 1} + 1 \leq 2^{2^n - 1} + 2^{2^n - 1} = 2^{2^n}, \end{aligned}$$

completing the proof. ■

A much stronger (and harder to prove) is that

$$\lim_{n \to \infty} \frac{n \log n}{p_n} = 1.$$

This is one of the equivalent formulations of the famous Prime Number Theorem.

Some famous open problems regarding the prime numbers are:

- (Goldbach's Conjecture) Is it true that every even number greater than two can be written as the sum of two prime numbers?
- Is it true that there are infinitely many primes p such that $p+2$ is a prime as well?

In some sense the Prime number Theorem and the above questions (in case of affirmative answers) say that there are many prime numbers. Here is a result which seems to say the opposite.

Theorem 4.6. *For every $n > 0$ there is a sequence of n consecutive composite numbers.*

Proof. Take for example $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$. ■