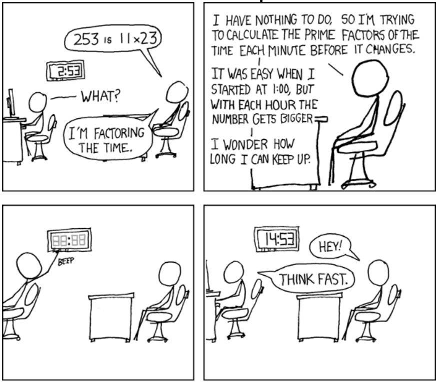
Discrete Mathematics

MATH1064, Lecture 13

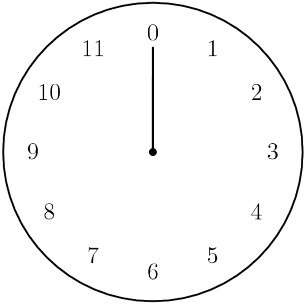
Jonathan Spreer



Extra exercises for Lecture 13

Section 4.1: Problems 1, 2, 5–10

Section 4.3: Problems 1–6, 16, 17, 24, 25



Questions

Consider the following statements:

A. $\forall a, b, m \in \mathbb{Z}$, if $m \mid a$ and $m \mid b$ then $m \mid (a + b)$.

B. $\forall a, b, m \in \mathbb{Z}$, if $m \mid a$ and $m \mid b$ then $m \mid (a - b)$.

C. $\forall a, b, m \in \mathbb{Z}$, if $m \mid a$ and $m \mid b$ then $m \mid (a \times b)$.

D. $\forall a, b, m \in \mathbb{Z}$, if $m \mid a$ and $m \mid b$ then $m \mid (a \div b)$.

Questions

Remember:

$n \equiv m \pmod{d}$

$\leftrightarrow d \mid (n - m)$

$\leftrightarrow$ n and m leave the same remainder when divided by d

From Lecture 12:

If $a \equiv b \pmod{d}$ and $n \equiv m \pmod{d}$, then

- $an \equiv bm \pmod{d}$,
- $a + n \equiv b + m \pmod{d}$, and
- $a - n \equiv b - m \pmod{d}$.

If $ac \equiv bc \pmod{d}$, is $a \equiv b \pmod{d}$?

Prime factorisation

Definition

The natural number $n \in \mathbb{N}$ is said to be written as a product of primes if there is a natural number $m \in \mathbb{N}$ and prime numbers $p_1, \dots, p_m$, such that

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_m = \prod_{k=1}^{m} p_k.$$

$42 = 2 \cdot 3 \cdot 7$
$21 = 3 \cdot 7$
$13 = 13$ (a trivial product of primes)
$24 = 2 \cdot 2 \cdot 2 \cdot 3$ (primes can be repeated)

Theorem (From Lecture 5)

Every natural number $n > 1$ can be written as a product of primes.

There is at least one prime!

Why? The “bounds for divisors” lemma shows that the only divisors of 2 are ± 1 and ± 2. So 2 is prime!

Proposition (Euclid)

There are infinitely many prime numbers.

Proof: Suppose to the contrary that there are only finitely many prime numbers, and label them $p_1, p_2, \ldots, p_n$.
Consider the number

$$m = p_1 p_2 \cdot \ldots \cdot p_n + 1 = 1 + \prod_{k=1}^{n} p_k.$$

Since 2 is prime, $m > 2 > 1$, and so m is a product of primes.
Therefore we can find some prime factor p of m; that is,
some prime p for which $p \mid m$.

Since p is prime and $p_1, p_2, \ldots, p_n$ is the list of all prime numbers, p must be equal to one of them.
Therefore p divides the product $\prod_{k=1}^{n} p_k$.

But: this product is just $m - 1$. So $p \mid m$ and $p \mid (m-1)$. Therefore p divides the difference $m - (m-1) = 1$; that is, $p \mid 1$.

From our "bounds for divisors" lemma we now have $0 < |p| \leq 1$, which means $|p| = 1$.
But 1 is not a prime number! This gives a contradiction.

Therefore there are infinitely many prime numbers. $\square$

Back to prime factorisation:

$$576 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$$
$$576 = 2 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$$
$$576 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 2 \cdot 2 \cdot 2$$
$$576 = 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$$
$$576 = 2^6 \cdot 3^2$$

The last line is the most compact and most informative!

The Fundamental Theorem of Arithmetic

Given any integer $n > 1$,
there exists a natural number k,
pairwise distinct prime numbers $p_1, p_2, \ldots p_k$,
and natural numbers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k} = \prod_{i=1}^{k} p_i^{e_i},$$

and any other expression for n as a product of prime numbers is identical to this except possibly for the order in which the factors are written.

The proof of unique factorisation is more difficult. You can read up on it in Section 5.2 (which is not part of this unit).

Applications of unique factorisation

What are all the positive divisors of 576?
We know $576 = 2^6 \cdot 3^2$.
The complete list of all $d \in \mathbb{N}$ for which $d \mid 576$ is:

$$
\begin{array}{lll}
2^6 \cdot 3^2 = 576 & 2^6 \cdot 3^1 = 192 & 2^6 \cdot 3^0 = 64 \\
2^5 \cdot 3^2 = 288 & 2^5 \cdot 3^1 = 96 & 2^5 \cdot 3^0 = 32 \\
2^4 \cdot 3^2 = 144 & 2^4 \cdot 3^1 = 48 & 2^4 \cdot 3^0 = 16 \\
2^3 \cdot 3^2 = 72 & 2^3 \cdot 3^1 = 24 & 2^3 \cdot 3^0 = 8 \\
2^2 \cdot 3^2 = 36 & 2^2 \cdot 3^1 = 12 & 2^2 \cdot 3^0 = 4 \\
2^1 \cdot 3^2 = 18 & 2^1 \cdot 3^1 = 6 & 2^1 \cdot 3^0 = 2 \\
2^0 \cdot 3^2 = 9 & 2^0 \cdot 3^1 = 3 & 2^0 \cdot 3^0 = 1
\end{array}
$$

So there are 21 positive divisors. They correspond to:

$$(7 \text{ choices for exponent of } 2) \times (3 \text{ choices for exponent of } 3)$$

Why is this list complete?

Because of unique prime factorisation.

Suppose $d \mid 576$ for some $d \in \mathbb{N}$. Then $d \cdot k = 576$ for some $k \in \mathbb{N}$.

Express d as a product of primes: $d = p_1 \ldots p_r$, and
express k as a product of primes: $k = q_1 \ldots q_s$.

Then $p_1 \ldots p_r \cdot q_1 \ldots q_s = 2^6 \cdot 3^2$,
and by unique prime factorisation, the list of primes $p_1, \ldots, p_r, q_1, \ldots, q_s$
is the same as the list $2, 2, 2, 2, 2, 2, 3, 3$,
possibly in a different order.

Therefore $d = 2^i \cdot 3^j$ with $0 \leq i \leq 6$ and $0 \leq j \leq 2$.

More applications of unique factorisation

For natural numbers a, b:

The greatest common divisor of the integers a and b (not both zero) is the largest $d \in \mathbb{N}$ for which $d \mid a$ and $d \mid b$.
We write this as $\gcd(a, b)$.

Example: $\gcd(9, 12) = 3, \quad \gcd(9, -12) = 3, \quad \gcd(0, -12) = 12$

The least common multiple of the positive integers a and b is the smallest $n \in \mathbb{N}$ for which $a \mid n$ and $b \mid n$.
We write this as $\mathrm{lcm}(a, b)$.

Examples: $\mathrm{lcm}(9, 12) = 36$

$$576 = 2^6 \cdot 3^2$$

$$78408 = 2^3 \cdot 3^4 \cdot 11^2$$

$\gcd(576, 78408) = 2^3 \cdot 3^2 = 72$
$\mathrm{lcm}(576, 78408) = 2^6 \cdot 3^4 \cdot 11^2 = 627264$

Computing the gcd

This is easy if you have prime factorisations!

$\gcd(2^4 \cdot 7^2 \cdot 13^2,\ -3^3 \cdot 7^3 \cdot 13) = 7^2 \cdot 13$
$\gcd(-2 \cdot 11^2,\ -3 \cdot 5) = 1$

Just take the smallest power of each prime that appears in both integers, and ignore any negative signs.

Lemma

If a and b are integers that are not both equal to zero, then $\gcd(a, b)$ *exists.*

Proof: Since $1 \mid a$ and $1 \mid b$, there is at least one common divisor.

Let $d \in \mathbb{Z}$ denote some common divisor of both a and b; that is, $d \mid a$ and $d \mid b$.

Without loss of generality, assume that $a \neq 0$.
By our "bounds on divisors" lemma from yesterday, $|d| \leq |a|$.
Therefore there are only finitely many common divisors, and so there exists a greatest common divisor. $\square$

Yet more applications of unique factorisation

Definition

Two integers $a, b \in \mathbb{Z}$ are called coprime if $\gcd(a, b) = 1$.

Lemma

If $a, b \in \mathbb{Z}$ are coprime and $ab = c^3$ for some $c \in \mathbb{Z}$, then $a = d^3$ and $b = e^3$ for some $d, e \in \mathbb{Z}$.

In words: If the product of two coprime integers is a cube, then each of the integers is a cube also.