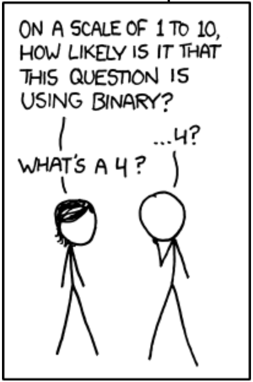
Discrete Mathematics

MATH1064, Lecture 14

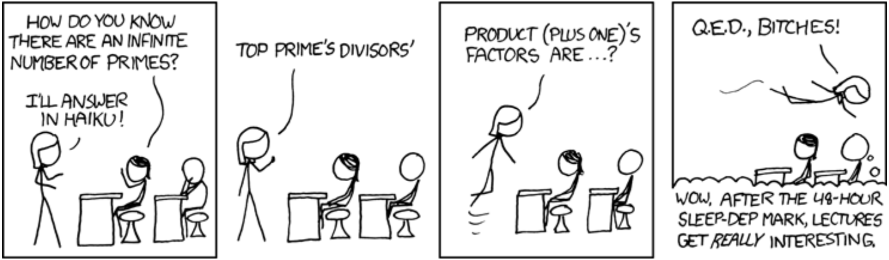
Jonathan Spreer



Extra exercises for Lecture 14

Section 4.2: Problems 1–∞

Section 4.3: Problems 32–36



Question:

Remember:

$n \equiv m \pmod{d}$

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

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

Statement S1

$6 \equiv 12 \pmod{6}$ and $2 \equiv 4 \pmod{6}$

Statement S2

$6 \equiv 21 \pmod{5}$ and $2 \equiv 7 \pmod{5}$

Equivalence is periodic

We can group integers into classes of numbers that are equivalent mod 5:

−10 −9 −8 −7 −6 **−5** −4 −3 −2 −1 **0** 1 2 3 4 **5** 6 7 8 9 **10**

−10 **−9** −8 −7 −6 −5 **−4** −3 −2 −1 0 **1** 2 3 4 5 **6** 7 8 9 10

−10 −9 **−8** −7 −6 −5 −4 **−3** −2 −1 0 1 **2** 3 4 5 6 **7** 8 9 10

−10 −9 −8 **−7** −6 −5 −4 −3 **−2** −1 0 1 2 **3** 4 5 6 7 **8** 9 10

−10 −9 −8 −7 **−6** −5 −4 −3 −2 **−1** 0 1 2 3 **4** 5 6 7 8 **9** 10

e.g., the second row says: $-9 \equiv -4 \equiv 1 \equiv 6 \pmod 5$

Why can we add?

Extra task from Lecture 12:

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

Proof. We use a direct proof. If $a \equiv b \pmod{d}$, then $d \mid (a - b)$. This means that $a - b = kd$ for some $k \in \mathbb{Z}$.
Likewise, if $n \equiv m \pmod{d}$, then $n - m = \ell d$ for some $\ell \in \mathbb{Z}$.

So:

$$(a + n) - (b + m) = a - b + n - m = kd + \ell d = (k + \ell)d.$$

Therefore $d \mid ((a + n) - (b + m))$, and so $a + n \equiv b + m \pmod{d}$. □

Exercise: Find similar proofs for $a - n \equiv b - m \pmod{d}$
and $an = bm \pmod{d}$!

Application: Calculations modulo 9

We have: $10 \equiv 1 \pmod 9$

By the above rules: $100 \equiv 10 \cdot 10 \equiv 1 \cdot 1 \equiv 1 \pmod 9$.

So in fact $10^k \equiv 1 \pmod 9$ for each $k \in \mathbb{N}$.

Choose any $n \in \mathbb{N}$, and name its digits: $n = a_m a_{m-1} \ldots a_1 a_0$.
(E.g. 438345 has $a_5 = 4, a_4 = 3, \ldots, a_0 = 5$)

Then $n = a_m 10^m + \ldots + a_1 10 + a_0$.
$(438345 = 400000 + 30000 + 8000 + 300 + 40 + 5 = 4 \cdot 10^5 + 3 \cdot 10^4 + \ldots)$

By the rules of modular arithmetic:

$$\begin{aligned} n &\equiv a_m 10^m + \ldots a_1 10 + a_0 \\ &\equiv a_m + \ldots + a_0 \qquad \pmod 9 \end{aligned}$$

So: $9 \mid n$ if and only if the sum of the digits of n is divisible by 9!

For 438345, we have $4 + 3 + 8 + 3 + 4 + 5 = 27 = 3 \cdot 9$,
and so 438345 is divisible by 9!

Back to computing the gcd

Remember: computing the gcd is easy is easy if you have prime factorisations!

Can we do this without prime factorisation?

Observation

For all $a, b \in \mathbb{Z}$, $\gcd(a, b) = \gcd(b, a - b)$.

Why?

- If $d \mid a$ and $d \mid b$, then $d \mid a - b$.
- If $d \mid b$ and $d \mid a - b$, then $d \mid b + (a - b) = a$.

So: the common divisors of a and b are the same as the common divisors of b and $a - b$!

In particular, the greatest common divisor of a and b is the same as the greatest common divisor of b and $a - b$.

Observation

For all $a, b \in \mathbb{Z}$, $\gcd(a, b) = \gcd(b, a - b)$.

How does this help? We can simplify the problem.

$\gcd(18, 14) =$

We can find the gcd without prime factorisation!

Can we speed this up?

Observation

For all $a, b \in \mathbb{Z}$, if $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

Why? Like before:

- If $d \mid a$ and $d \mid b$, then $d \mid bq$ and so $d \mid a - bq$. Thus $d \mid r$.
- If $d \mid r$ and $d \mid b$, then $d \mid bq$ and so $d \mid bq + r$. Thus $d \mid a$.

So again: the common divisors of a and b are the same as the common divisors of b and r!

In particular, the greatest common divisor of a and b is the same as the greatest common divisor of b and r.

Does this help?

Observation

For all $a, b \in \mathbb{Z}$, if $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

We can simplify the problem more quickly:

For $\gcd(18, 14)$:

a	b	Divide by b	r	Result
18	14	$18 = 1 \cdot 14 + 4$	4	$\gcd(18, 14) = \gcd(14, 4)$
14	4	$14 = 3 \cdot 4 \ \ + 2$	2	$\gcd(14, 4) = \gcd(4, 2)$
4	2	$4 = 2 \cdot 2 \ \ + 0$	0	$\gcd(4, 2) = \gcd(2, 0)$

and $\gcd(2, 0) = 2$. Therefore $\gcd(18, 14) = 2$!

This process is called the Euclidean algorithm.

The Euclidean algorithm

To find $\gcd(a, b)$ where $a, b \in \mathbb{Z}$ and $a \geq b > 0$:

- Write $a = qb + r$, as in the quotient-remainder theorem;
- If $r = 0$, then terminate with $\gcd(a, b) = b$;
- Otherwise, replace (a, b) by (b, r) and repeat!

Notice that the gcd is the last non-zero remainder.

Could this process repeat forever?

No! By the quotient-remainder theorem, $0 \leq r < b$.
Since we use the old value of r as the new value of b when we repeat, this means that r becomes strictly smaller on each repetition.

Therefore we must eventually reach $r = 0$ and terminate!

Question

What is the gcd of 18 and 11064 ?

$$\begin{aligned} 11064 &= 614 \cdot 18 + 12 \\ 18 &= 1 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 + 0 \end{aligned}$$

Therefore $\gcd(18, 11064) = 6$.

We've only discussed $a, b \geq 0$. What about arbitrary $a, b \in \mathbb{Z}$?

- If one or both of a, b are negative, then just ignore the negative signs: $\gcd(a, b) = \gcd(|a|, |b|)$.
- If $a = 0$ and $b = 0$, then $\gcd(a, b)$ is not defined.
- If $a \neq 0$ and $b = 0$, then $\gcd(a, b) = |a|$.
- If $a = 0$ and $b \neq 0$, then $\gcd(a, b) = |b|$.

Greatest common divisors and the Euclidean algorithm are extremely important in modern cryptography.

Go and read about the RSA encryption system!

Representation of integers

Theorem (Base b expansion)

Let b be an integer greater than 1. Every positive integer n can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0,$$

where k is a non-negative integer, $a_0, \ldots, a_k$ are non-negative integers less than b and $a_k \neq 0$.

Example and notation:
Base 2: $165 =$
Base 8: $165 =$
Base 16: $165 =$
For hexadecimal (base 16), one usually uses the digits
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

An algorithm to write a number in base b

- Repeatedly divide by b, and write down the remainders
- Stop when you reach zero
- The remainders will give the digits in reverse order

Example: What is $(78)_{10}$ in base 2?

$(78)_{10} =$

Addition and multiplication

Base b uses a positional system, and so you can add and subtract as usual!

Example:

In base 7, $(36)_7 + (144)_7 =$

In base 2, $(110)2 + (111)2 =$

In base 2, $(111)2 \times (11)2 =$

Question

I'm thinking of an integer $n > 1$ (but I won't tell you what it is).

What is n when written in base n?

1. $(0)_n$
2. $(1)_n$
3. $(10)_n$
4. $(11)_n$
5. $(100\ldots0)_n$, with n zeroes
6. I cannot answer this without knowing the value of n