Math 235 Fall 2024, Lecture 3 stenogram: Induction and modular arithmetic

website: `https://www.cip.ifi.lmu.de/~grinberg/t/24f`

1. Number Theory I: Divisibility and congruence

Number theory is one of the oldest parts of mathematics, and it is often taught in undergraduate proofs classes and even in high school. I will thus mostly summarize the results, and refer for proofs to the notes. The topic of prime numbers will be omitted as well, since I want to keep it for a later week.

1.1. Divisibility

From now on, $\mathbb{N}$ shall mean $\{0, 1, 2, \ldots\}$.

Definition 1.1.1. Given two integers a and b, we write "$a \mid b$" (and say "a **divides** b" or "b is **divisible** by a" or "b is a **multiple** of a" or "a is a **divisor** of b") if there exists an integer c such that $b = ac$.

We write "$a \nmid b$" for "not $a \mid b$".

Theorem 1.1.2 (Divisibility facts)**.** In the following, all unspecified variables are integers.

(a) We have $a \mid 0$ for any $a \in \mathbb{Z}$. In particular, $0 \mid 0$.

(b) But $0 \mid b$ holds only for $b = 0$.

(c) We always have $a \mid a$.

(d) Signs do not matter in divisibility: i.e., we have $a \mid b$ if and only if $|a| \mid |b|$.

(e) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$. (When a and b are positive, this is just saying: If $a \mid b$, then $a \leq b$.)

(f) If $a \mid b$ and $b \mid a$, then $|a| = |b|$.

(g) If $a \neq 0$, then $a \mid b$ is equivalent to $\dfrac{b}{a} \in \mathbb{Z}$.

(h) If $a \mid b$ and $b \mid c$, then $a \mid b \mid c$.

(i) If $a_1 \mid b_1$ and $a_2 \mid b_2$, then $a_1 a_2 \mid b_1 b_2$.

(j) If $a \mid b$, then $a^k \mid b^k$ for any $k \in \mathbb{N}$.

(k) We have $a \mid b$ if and only if $ac \mid bc$, as long as $c \neq 0$.

(l) If $a \mid b$ and $a \mid c$, then $a \mid b + c$ and $a \mid b - c$.

1.2. Modular arithmetic: Congruences

Congruences (more precisely, **modular congruences**) are just reformulated divisibilities. Nevertheless, the reformulation is useful, since it exposes their most useful qualities.

Definition 1.2.1. Let $n, a, b \in \mathbb{Z}$. We say that a **is congruent to** b **modulo** n, and we write "$a \equiv b \bmod n$", if and only if $n \mid a - b$.
We write "$a \not\equiv b \bmod n$" for "not $a \equiv b \bmod n$".
Statements of the form "$a \equiv b \bmod n$" are called **congruences**.

For example, $3 \equiv 9 \bmod 2$ since $3 - 9 = -6$ is a multiple of 2. But $3 \not\equiv 6 \bmod 2$ since $3 - 6$ is not a multiple of 2. We have $a \equiv b \bmod 0$ if and only if $a = b$. We have $a \equiv b \bmod 1$ always.

Theorem 1.2.2 (Congruence facts)**.** Again, all unspecified variables shall be integers.
(a) We have $a \equiv 0 \bmod n$ if and only if $n \mid a$.
(b) We have $a \equiv b \bmod n$ if and only if there exists $d \in \mathbb{Z}$ such that $a = b + nd$.
(c) We always have $a \equiv a \bmod n$.
(d) If $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$.
(e) If $a \equiv b \bmod n$, then $b \equiv a \bmod n$.
(f) We have $a - b \equiv c \bmod n$ if and only if $a \equiv b + c \bmod n$.
(g) If $a_1 \equiv b_1 \bmod n$ and $a_2 \equiv b_2 \bmod n$, then

$$\begin{aligned} a_1 + a_2 &\equiv b_1 + b_2 \bmod n; \\ a_1 - a_2 &\equiv b_1 - b_2 \bmod n; \\ a_1 a_2 &\equiv b_1 b_2 \bmod n. \end{aligned}$$

That is, congruences modulo the same n can be added, subtracted and multiplied at will. (But not divided.)
(h) If $a \equiv b \bmod n$, then $a^k \equiv b^k \bmod n$ for any $k \in \mathbb{N}$.
(i) If $a \equiv b \bmod n$ and $m \mid n$, then $a \equiv b \bmod m$.

These facts are not hard to prove (see notes), but already quite useful. Here is an example:

Exercise 1. Let $n \in \mathbb{N}$. Show that $7 \mid 3^{2n+1} + 2^{n+2}$.

Solution. Equivalently, we must prove that $3^{2n+1} + 2^{n+2} \equiv 0 \bmod 7$.
We can try to simplify the LHS (left hand side) modulo 7. We have

$$3^{2n+1} = \left(\underbrace{3^2}_{=9 \equiv 2 \bmod 7} \right)^n \cdot 3 \equiv 2^n \cdot 3 \bmod 7.$$

The reason why we are allowed to do this is some of the above congruence rules: We are really arguing that $3^2 \equiv 2 \bmod 7$, so $\left(3^2\right)^n \equiv 2^n \bmod 7$, and multiplying this by the congruence $3 \equiv 3 \bmod 7$, we get $\left(3^2\right)^n \cdot 3 \equiv 2^n \cdot 3 \bmod 7$.

On the other hand,

$$2^{n+2} \equiv 2^n \cdot 4 \bmod 7$$

(actually an equality, not just a congruence). Adding these two congruences together, we obtain

$$3^{2n+1} + 2^{n+2} \equiv 2^n \cdot 3 + 2^n \cdot 4 = 2^n \cdot \underbrace{7}_{\equiv 0 \bmod 7} \equiv 2^n \cdot 0 = 0 \bmod 7.$$

And we are done. ■

As we saw in the above proof, congruences can be substituted into each other: For example, if $a \equiv b \bmod n$, then

$$(a+2)(a+9) - a \equiv (b+2)(b+9) - b \bmod n.$$

Formally, this is obtained by adding the congruence $a \equiv b \bmod n$ to the trivial congruences $2 \equiv 2 \bmod n$ and $9 \equiv 9 \bmod n$, then multiplying, then subtracting, and so on.

This kind of substitution makes congruences particularly useful: They encode divisibilities, yet they are as easy to handle as equalities. Just be careful: You can only substitute in "polynomial expressions" (i.e., in expressions with $+$, $-$ and $\cdot$). You cannot substitute in exponents: e.g., $a \equiv b \bmod n$ does not imply $2^a \equiv 2^b \bmod n$. But we can substitute in bases of exponents: e.g., $a \equiv b \bmod n$ implies $a^2 \equiv b^2 \bmod n$.

When substituting b for a, you don't have to replace all a's by b's; you can leave some a's unchanged.

Exercise 2. Let $(f_0, f_1, f_2, \ldots)$ be the Fibonacci sequence. Prove that if $a, b \in \mathbb{N}$ satisfy $a \mid b$, then $f_a \mid f_b$.

Solution. Writing b as $b = ac$ for some $c \in \mathbb{N}$, we can rewrite this as follows: Prove that every $a, c \in \mathbb{N}$ satisfy $f_a \mid f_{ac}$.

Now we need to prove this. We induct on c.

The *base case* ($c = 0$) is easy: $f_{ac} = f_{a \cdot 0} = f_0 = 0$ is divisible by everything.

Induction step: Assume that $f_a \mid f_{ac}$. We must show that $f_a \mid f_{a(c+1)}$.

We have

$$\begin{aligned}
f_{a(c+1)} &= f_{ac+a} = f_{ac+(a-1)+1} \\
&= f_{ac} f_{a-1} + f_{ac+1} f_{(a-1)+1} \qquad \left(\begin{array}{c} \text{by the addition formula for Fibonacci numbers} \\ \text{(Exercise 5 in Lecture 1)} \end{array} \right) \\
&= \underbrace{f_{ac}}_{\substack{\equiv 0 \bmod f_a \\ \text{(since } f_a \mid f_{ac}\text{)}}} f_{a-1} + f_{ac+1} \underbrace{f_a}_{\substack{\equiv 0 \bmod f_a \\ \text{(since } f_a \mid f_a\text{)}}} \\
&\equiv 0 f_{a-1} + f_{ac+1} 0 = 0 \bmod f_a,
\end{aligned}$$

so that $f_a \mid f_{a(c+1)}$, and we are done (with the induction step and thus the whole proof).

Not so fast: We applied the addition formula to ac and $a-1$ in the roles of n and m. This requires $ac \geq 0$ and $a-1 \geq 0$. Well, $ac \geq 0$ is clear, but $a-1 \geq 0$ holds only for $a \geq 1$. So the case $a = 0$ must be handled separately. But it is obvious anyway ($a = 0$ implies $ac = 0$, thus $f_{ac} = 0$). ■

1.3. Quotients and remainders

One of the "workhorse results" in elementary number theory is division with remainder:

Theorem 1.3.1 (division with remainder theorem)**.** Let n be a positive integer. Let u be any integer. Then, there exists a unique pair (q, r) with $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$ and $u = qn + r$.

Definition 1.3.2. Consider this pair (q, r).

Its first entry q is denoted $u//n$ and called the **quotient of the division of u by n**.

Its second entry r is denoted $u\%n$ and called the **remainder of the division of u by n**.

Other authors use other notations. A lot of people write $u \bmod n$ for $u\%n$, but this is sketchy ($u \bmod n$ more standardly means the residue class of u modulo n, which is the set of all integers that are congruent to u modulo n).

The theorem is not hard to prove by induction on u. The only twist is that u can be negative, so you need a version of induction that can go both up and down (i.e., with two induction steps: $u \mapsto u+1$ and $u \mapsto u-1$); I call this "**two-sided induction**". Alternatively, you can use regular induction to cover the case $u \geq 0$ and then some other trick to extend it to negative u.

Theorem 1.3.3 (Division with remainder facts)**.** Let n be a positive integer, and $u, v \in \mathbb{Z}$.

(a) We have $u\%n \in \{0, 1, \ldots, n-1\}$ and $u\%n \equiv u \bmod n$ and $u = (u//n)\, n + (u\%n)$.

(b) We have $n \mid u$ if and only if $u\%n = 0$.

(c) If $c \in \{0, 1, \ldots, n-1\}$ is such that $c \equiv u \bmod n$, then $c = u\%n$.

(d) We have $u//n = \left\lfloor \dfrac{u}{n} \right\rfloor$, where $\lfloor x \rfloor$ means the floor of x.

(e) We have $u \equiv v \bmod n$ if and only if $u\%n = v\%n$.

(f) We have

$$(u \text{ is even}) \iff (2 \mid u) \iff (u \equiv 0 \bmod 2) \iff (u\%2 = 0)$$

and

$$(u \text{ is odd}) \iff (2 \nmid u) \iff (u \equiv 1 \bmod 2) \iff (u\%2 = 1).$$

These facts are fundamental. Even things that are completely obvious (such as "the sum of any two odd integers is even") are proved using them. But also some less obvious things, such as the following:

Exercise 3. Let n be an odd integer. Prove that $8 \mid n^2 - 1$.

Solution. Since n is odd, we have $n \equiv 1 \bmod 2$ (by the above facts). Thus, $n = 2k + 1$ for some $k \in \mathbb{Z}$. Consider this k. Now,

$$n^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4\left(k^2 + k\right) = 4k(k+1).$$

If we can show that $2 \mid k(k+1)$, then we are therefore done (since the 2 joins the 4 factor to obtain $2 \cdot 4 = 8$). So why is $2 \mid k(k+1)$? Because

- if k is even, then $2 \mid k \mid k(k+1)$;
- if k is odd, then $k \equiv 1 \bmod 2$, so that $k + 1 \equiv 1 + 1 = 2 \equiv 0 \bmod 2$, so that $2 \mid k + 1 \mid k(k+1)$.

So we are done. ■

Exercise 4. Let n be an integer such that $3 \nmid n$. Prove that $3 \mid n^2 - 1$.

Solution. We want to show that $n^2 \equiv 1 \bmod 3$. But the above facts tell us that $n\%3 \equiv n \bmod 3$, so that $n \equiv n\%3 \bmod 3$. So we can replace n by $n\%3$ in the congruence that we are trying to prove.

But $n\%3$ is either 0 or 1 or 2, and cannot be 0 (since $3 \nmid n$). So $n\%3$ is either 1 or 2. Hence, instead of proving that $n^2 \equiv 1 \bmod 3$, we only need to show that $1^2 \equiv 1 \bmod 3$ and $2^2 \equiv 1 \bmod 3$. But this is straightforward ($1^2 = 1$ and $2^2 = 4 \equiv 1 \bmod 3$). ■

What we have done in this solution is a general technique: the "try all possible remainders" method for proving divisibilities and congruences. We could also do the previous exercise ($8 \mid n^2 - 1$) in the same way, but we would have to try all possible remainders upon division by 8, of which there are only 4 (since the odd number n must leave an odd remainder, i.e., one of $1, 3, 5, 7$). Likewise, we can show that any integer n satisfies $6 \mid n^3 - n$ and $12 \mid n^4 - n^2$ and $24 \mid n^5 - n^3$ and $6 \mid n(n+1)(n+2)$ and many other such claims.

Another example of the use of congruence arguments:

Exercise 5. Which Fibonacci numbers are even?

Solution. See whiteboard, and see the notes for the formal version. Essentially, the idea is to compute the remainders $f_n\%2$ by interpreting the recursion $f_n = f_{n-1} + f_{n-2}$ modulo 2. The sequence of remainders is periodic with period 3, and we conclude that f_n is even if and only if $3 \mid n$. ■

1.4. Greatest common divisors

Definition 1.4.1. A **common divisor** of k integers $b_1, b_2, \ldots, b_k$ is an integer a such that

$$a \mid b_i \qquad \text{for each } i \in \{1, 2, \ldots, k\}.$$

For example, the common divisors of 6 and 8 are $-2, -1, 1, 2$.

Definition 1.4.2. The **greatest common divisor** (short: **gcd**) of k integers $b_1, b_2, \ldots, b_k$ is defined as follows:

- If not all of $b_1, b_2, \ldots, b_k$ are 0, then it is literally the largest of all common divisors of $b_1, b_2, \ldots, b_k$.
- If all of $b_1, b_2, \ldots, b_k$ are 0, then it is 0 by decree.

We denote it by $\gcd(b_1, b_2, \ldots, b_k)$.

Theorem 1.4.3 (Basic gcd facts)**.** All variables here are understood to be integers.
(a) We have $\gcd(a, b) = \gcd(b, a)$.
(b) We have $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$.
(c) We have $\gcd(a, 0) = \gcd(0, a) = |a|$.
(d) We have $\gcd(a, ua + b) = \gcd(a, b)$. (This is the basic tool behind the Euclidean algorithm.)
(e) If $b \equiv c \bmod a$, then $\gcd(a, b) = \gcd(a, c)$. (In other words, in a gcd of two numbers, we can move one by a multiple of the other.)
(f) If $a > 0$, then $\gcd(a, b) = \gcd(a, b\%a)$.
(g) We have $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b)$.
(h) If $a \mid b$, then $\gcd(a, b) = |a|$.
(i) We have $\gcd() = 0$.

These facts can be very useful for finding gcds without having to decompose the numbers into prime factors ("**Euclidean algorithm**"). For instance,

$$\begin{aligned}
\gcd(21, 34) &= \gcd(21, 13) \qquad (\text{since } 34\%21 = 13) \\
&= \gcd(13, 21) = \gcd(13, 8) = \gcd(8, 13) = \gcd(8, 5) \\
&= \gcd(5, 8) = \gcd(5, 3) = \gcd(3, 5) = \gcd(3, 2) \\
&= \gcd(2, 3) = \gcd(2, 1) = \gcd(1, 2) = \gcd(1, 0) = |1| = 1.
\end{aligned}$$

Note that these are the Fibonacci numbers, unsurprisingly because $f_{n+1}\%f_n = f_{n-1}$ for all $n \geq 1$. Thus we have really shown the following:

Proposition 1.4.4. The gcd of any two consecutive Fibonacci numbers is 1. That is, $\gcd(f_n, f_{n+1}) = 1$ for the Fibonacci sequence and any $n \in \mathbb{N}$.

Now to some more significant and less obvious properties of gcds:

Theorem 1.4.5 ("Advanced" gcd facts)**. (a) Bezout's theorem:** For any two integers a and b, there exist integers x and y such that

$$\gcd(a, b) = xa + yb.$$

In other words, $\gcd(a, b)$ is always a linear combination of a and b with integer coefficients.

(b) The universal property of the gcd: For any three integers m, a, b, the equivalence

$$(m \mid a \text{ and } m \mid b) \iff (m \mid \gcd(a, b))$$

holds. In other words, the common divisors of a and b are precisely the divisors of $\gcd(a, b)$.

(c) For any $s, a, b \in \mathbb{Z}$, we have

$$\gcd(sa, sb) = |s| \gcd(a, b).$$

(d) If $a_1 \mid b_1$ and $a_2 \mid b_2$, then

$$\gcd(a_1, a_2) \mid \gcd(b_1, b_2).$$

Proofs can be found in the notes. Main idea for **(a)**: induction. But first, replace a and b by $|a|$ and $|b|$, so that a and b become nonnegative. Then, do strong induction on $a + b$. In the induction step, reduce the problem for (a, b) to either the problem for $(a - b, b)$ (if $a \geq b$) or the problem for $(a, b - a)$ (if $a \leq b$). In either case, the sum $a + b$ goes down, unless one of a, b is 0, but this case is easy. This inductive proof leads to the **Extended Euclidean algorithm** for finding the x and the y. Part **(b)** can be derived from **(a)**, and parts **(c)** and **(d)** can be derived from **(b)**.

Most of the above can be generalized to multiple numbers:

Theorem 1.4.6 ("Advanced" gcd facts)**. (a) Bezout's theorem:** For any k integers $a_1, a_2, \ldots, a_k$, there exist integers $x_1, x_2, \ldots, x_k$ such that

$$\gcd(a_1, a_2, \ldots, a_k) = x_1a_1 + x_2a_2 + \cdots + x_ka_k.$$

In other words, $\gcd(a_1, a_2, \ldots, a_k)$ is always a linear combination of $a_1, a_2, \ldots, a_k$ with integer coefficients.

(b) The universal property of the gcd: For any integers $m, a_1, a_2, \ldots, a_k$, the equivalence

$$(m \mid a_i \text{ for all } i \in \{1, 2, \ldots, k\}) \iff (m \mid \gcd(a_1, a_2, \ldots, a_k))$$

holds. In other words, the common divisors of $a_1, a_2, \ldots, a_k$ are precisely the divisors of $\gcd(a_1, a_2, \ldots, a_k)$.

(c) For any $s, a_i \in \mathbb{Z}$, we have

$$\gcd(sa_1, sa_2, \ldots, sa_k) = |s| \gcd(a_1, a_2, \ldots, a_k).$$

(d) If $a_i \mid b_i$ for all i, then

$$\gcd(a_1, a_2, \ldots, a_k) \mid \gcd(b_1, b_2, \ldots, b_k).$$

(e) Associativity: We have

$$\begin{aligned}&\gcd(b_1, b_2, \ldots, b_k, c_1, c_2, \ldots, c_\ell) \\ &= \gcd(\gcd(b_1, b_2, \ldots, b_k), \gcd(c_1, c_2, \ldots, c_\ell)).\end{aligned}$$

Exercise 6. Let u be an integer, and $a, b \in \mathbb{N}$. Prove that

$$\gcd\left(u^a - 1,\ u^b - 1\right) = \left|u^{\gcd(a,b)} - 1\right|.$$

Solution. Exercise 3.4.1 in the notes. Recommend looking at the solution there. The crux of the argument is: When you subtract the smaller of a and b from the larger, both sides of the claim are unchanged. (For the right hand side, this follows from $\gcd(a, b) = \gcd(a - b, b)$, but for the left hand side it requires more work.) This allows you to gradually reduce the problem to the case when a or b is 0 (formally, this is a strong induction on $a + b$).

1.5. Coprimality

Gcds are at their most useful when they equal 1. This has a name:

Definition 1.5.1. Two integers a and b are said to be **coprime** (and I write "$a \perp b$" for this) if $\gcd(a, b) = 1$.

This is clearly a symmetric relation. "Coprime" is also known as "relatively prime" (or "prime to each other", but please avoid this one).

For example, 2 is coprime to 3, since $\gcd(2,3) = 1$. More generally, each a is coprime to $a+1$, since $\gcd(a, a+1) = \gcd(a,1) = 1$.

When is a coprime to $a+2$? When a is odd. Indeed,

$$\gcd(a, a+2) = \gcd(a,2) = \begin{cases} 2, & \text{if } a \text{ is even;} \\ 1, & \text{if } a \text{ is odd.} \end{cases}$$

Any number a is coprime to 1, but only 1 and -1 are coprime to 0.

Theorem 1.5.2 (Coprimality facts)**.** All variables here are integers.

(a) Cancellation from divisibility: If $a \mid bc$ and $a \perp b$, then $a \mid c$. You can think of this rule as a way to remove "unsolicited guests" from a divisibility. (Here, the guest is b.)

(b) Combining two divisibilities: If $a \mid c$ and $b \mid c$ and $a \perp b$, then $ab \mid c$.

(c) If $a_1 \mid b_1$ and $a_2 \mid b_2$ and $b_1 \perp b_2$, then $a_1 \perp a_2$.

(d) If $a \perp c$ and $b \perp c$, then $ab \perp c$.

(e) If $a_i \perp c$ for all $i \in \{1, 2, \ldots, k\}$, then $a_1 a_2 \cdots a_k \perp c$.

(f) If $a \perp b$, then $a^n \perp b^m$ for all $n, m \in \mathbb{N}$.

(g) Combining k divisibilities: If $a_1, a_2, \ldots, a_k$ are k mutually coprime divisors of c, then $a_1 a_2 \cdots a_k \mid c$. **Caution:** "Mutually coprime" means that $a_i \perp a_j$ for all $i \neq j$, not that $\gcd(a_1, a_2, \ldots, a_k) = 1$.

(h) Cancellation from congruence: If $a \perp n$ and $ab \equiv ac \bmod n$, then $b \equiv c \bmod n$.

(i) Reducing fractions: If $(a,b) \neq (0,0)$ and $g = \gcd(a,b)$, then $g > 0$ and $\dfrac{a}{g} \perp \dfrac{b}{g}$. This is saying that any fraction $\dfrac{a}{b}$ of integers can be brought to a reduced form by cancelling the gcd of numerator and denominator.

Caution: It is easy to find three integers x, y, z that satisfy $\gcd(x,y,z) = 1$ but that are not mutually coprime. Indeed, taking $x = 6$ and $y = 10$ and $z = 15$, we note that $\gcd(x,y,z) = 1$ but no two of x, y, z are coprime.