Math 221 Winter 2023, Lecture 10: Elementary number theory

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wd`

3. Elementary number theory

3.4. Greatest common divisors (cont'd)

Last time, we proved two important properties of gcds:

Theorem 3.4.5 (Bezout's theorem for integers)**.** Let a and b be two integers. Then, there exist two integers x and y such that

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

Theorem 3.4.8 (universal property of the gcd)**.** Let $a, b, m \in \mathbb{Z}$. Then, we have the equivalence

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

We note that Theorem 3.4.8 is commonly used in the "$\Longrightarrow$" direction (since the "$\Longleftarrow$" direction is trivial). That is, the following fact is used most of the time:

Corollary 3.4.9 (universal property of the gcd, forward direction)**.** Let $a, b, m \in \mathbb{Z}$. If $m \mid a$ and $m \mid b$, then $m \mid \gcd(a,b)$.

Proof. This is the "$\Longrightarrow$" direction of Theorem 3.4.8. □

3.4.6. Factoring out a common factor from a gcd

The following theorem has an "intuitively obvious" feel, but its proof is not as simple as you might suspect:

Theorem 3.4.10. Let $s, a, b \in \mathbb{Z}$. Then,

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

This is saying that when two integers have a common factor s, then this common factor can be pulled out of their gcd. (The caveat is, of course, that the common factor must be replaced by its absolute value, since a gcd cannot be negative by definition.)

Proof of Theorem 3.4.10. Let

$$g = \gcd(a, b) \qquad \text{and} \qquad h = \gcd(sa, sb).$$

Thus, we must prove that $h = |s| \cdot g$. Note that h and g are nonnegative (because Proposition 3.4.3 **(a)** from Lecture 9 shows that gcds are always nonnegative). Thus, $h = |h|$ and $g = |g|$, so that $|s| \cdot g = |s| \cdot |g| = |sg|$ (since $|x| \cdot |y| = |xy|$ for any two real numbers x and y).

Our goal is to prove that $h = |s| \cdot g$. Since $h = |h|$ and $|s| \cdot g = |sg|$, this amounts to proving that $|h| = |sg|$. So this is our goal now.

One good way to prove that two integers p and q satisfy $|p| = |q|$ is by showing that $p \mid q$ and $q \mid p$. Indeed, from $p \mid q$ and $q \mid p$, it follows that $|p| = |q|$ (by Proposition 3.1.4 **(c)** in Lecture 7).

Thus, in order to prove that $|h| = |sg|$, it will suffice to show that $h \mid sg$ and $sg \mid h$. Now, let us do this.

- *Proof of $sg \mid h$:* We have $g = \gcd(a, b) \mid a$. Multiplying both sides by s, we thus obtain $sg \mid sa$ [1]. Similarly, $sg \mid sb$. Hence, Corollary 3.4.9 (applied to sg, sa and sb instead of m, a and b) yields $sg \mid \gcd(sa, sb)$. In other words, $sg \mid h$ (since $h = \gcd(sa, sb)$).

- *First proof of $h \mid sg$:* If $s = 0$, then the claim $h \mid sg$ is obvious (since $\underbrace{s}_{=0} g = 0 = h \cdot 0$). Thus, let us consider the case when $s \neq 0$.

  We have just showed that $sg \mid h$, but we also clearly have $s \mid sg$. Thus, $s \mid sg \mid h$. Since $s \neq 0$, this entails that $\dfrac{h}{s} \in \mathbb{Z}$ (by Proposition 3.1.4 **(d)** in Lecture 7, applied to s and h instead of a and b).

  This integer $\dfrac{h}{s}$ satisfies $s \cdot \dfrac{h}{s} = h = \gcd(sa, sb) \mid sa$. Dividing both sides by s, we thus obtain $\dfrac{h}{s} \mid a$ [2]. Similarly, $\dfrac{h}{s} \mid b$. Hence, Corollary 3.4.9 (applied to $m = \dfrac{h}{s}$) yields $\dfrac{h}{s} \mid \gcd(a, b)$. In other words, $\dfrac{h}{s} \mid g$ (since $g = \gcd(a, b)$). Multiplying both sides by s, we thus obtain $s \cdot \dfrac{h}{s} \mid sg$. In other words, $h \mid sg$. Thus, $h \mid sg$ is proved.

- *Second proof of $h \mid sg$:* We have $h = \gcd(sa, sb) \mid sa$. In other words, $sa = hu$ for some integer u. Similarly, $sb = hv$ for some integer v. Consider these integers u and v.

[1] "Multiplying both sides by s" means using the following simple fact: If two integers x and y satisfy $x \mid y$, then $sx \mid sy$.

[2] "Dividing both sides by s" means using the following simple fact: If two integers x and y satisfy $sx \mid sy$, then $x \mid y$. (Note that this relies on $s \neq 0$.)

However, Bezout's theorem (Theorem 3.4.5) shows that there exist two integers x and y such that $\gcd(a,b) = xa + yb$. Consider these x and y.

Now, $g = \gcd(a,b) = xa + yb$, so that

$$sg = s(xa+yb) = sxa + syb = \underbrace{sa}_{=hu} x + \underbrace{sb}_{=hv} y = hux + hvy = h\underbrace{(ux+vy)}_{\text{an integer}}.$$

This again proves that $h \mid sg$.

We have now proved that $h \mid sg$ (proved in two different ways) and $sg \mid h$. Hence, as explained above, we obtain $|h| = |sg|$. As we also explained above, this completes our proof of Theorem 3.4.10. □

3.5. Coprime integers

3.5.1. Definition and examples

Greatest common divisors are at their most useful when they are 1. This is called "coprimality":

Definition 3.5.1. Two integers a and b are said to be **coprime** (or **relatively prime**) if $\gcd(a,b) = 1$.

Remark 3.5.2. This is a symmetric relation: If a and b are coprime, then b and a are coprime (since $\gcd(b,a) = \gcd(a,b)$).

Example 3.5.3. (a) An integer n is coprime to 2 if and only if n is odd. Indeed, we know that $\gcd(n,2)$ is a divisor of 2 and is a nonnegative integer (since any gcd is a nonnegative integer). Thus, $\gcd(n,2)$ must be either 1 or 2 (since the only nonnegative divisors of 2 are 1 and 2). Now:

- If $\gcd(n,2) = 2$, then n is even (since $2 = \gcd(n,2) \mid n$).
- If $\gcd(n,2) = 1$, then n is odd (because otherwise, 2 would be a common divisor of n and 2, but this cannot happen when the greatest common divisor of n and 2 is 1).

(b) An integer n is coprime to 3 if and only if n is not divisible by 3. (This can be proved just as part **(a)**, since the only nonnegative divisors of 3 are 1 and 3.)

(c) An integer n is coprime to 4 if and only if n is odd. (If you expected "... if n is not divisible by 4" here, then you were wrong. The nonnegative divisors of 4 are not only 1 and 4 but also 2.)

(d) An integer n is coprime to 5 if and only if n is not divisible by 5. (This can be proved just as part **(a)**, since the only nonnegative divisors of 5 are 1 and 5.)

Informally, I think of coprimality as some sort of "unrelatedness" or "independence" or "orthogonality" or "noninterference" relation. In other words, two integers a and b are coprime if and only if they have "nothing to do with each other", in some sense. This is nowhere near a rigorous statement, but it motivates many properties of coprimality, including the ones we will see below.

3.5.2. Three theorems about coprimality

The following three theorems are useful properties of coprime integers:

Theorem 3.5.4 (coprime divisors theorem)**.** Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid c$ and $b \mid c$. Assume that a and b are coprime. Then, $ab \mid c$.

(In other words, a product of two coprime divisors of c is again a divisor of c.)

Proof. We have $ab \mid ac$ (since $b \mid c$) and $ba \mid bc$ (because $a \mid c$). Since $ba = ab$ and $ac = ca$ and $bc = cb$, we can rewrite this as follows: We have $ab \mid ca$ and $ab \mid cb$. Thus, Corollary 3.4.9 (applied to ab, ca and cb instead of m, a and b) yields

$$ab \mid \gcd(ca, cb) = |c| \cdot \underbrace{\gcd(a, b)}_{\substack{=1 \\ \text{(since } a \text{ is coprime to } b\text{)}}} \qquad \text{(by Theorem 3.4.10)}$$
$$= |c| .$$

Since divisibility does not depend on signs (Proposition 3.1.4 **(a)** in Lecture 7), we thus obtain $ab \mid c$ [3]. This proves Theorem 3.5.4. □

Example 3.5.5. We have $4 \mid 56$ and $7 \mid 56$. Since 4 and 7 are coprime, we can thus conclude (by Theorem 3.5.4, applied to $a = 4$, $b = 7$ and $c = 56$) that $4 \cdot 7 \mid 56$.

In contrast, from $6 \mid 12$ and $4 \mid 12$, we cannot conclude that $6 \cdot 4 \mid 12$, since 6 and 4 are not coprime.

In terms of our "coprimality as independence" heuristic, Theorem 3.5.4 can be made intuitive as follows: If a and b are two coprime divisors of c, then (because a and b are coprime) a and b must divide "different parts" of c, and thus their product ab is still a divisor of c. Of course, the notion of "different parts" here is not a real thing, but it is helpful as a mnemonic device.

[3] Here is this argument in detail: We have just proved that $ab \mid \operatorname{abs} c$ (where we write $\operatorname{abs} x$ for $|x|$ in order to avoid confusing absolute-value bars with divisibility symbols). Proposition 3.1.4 **(a)** in Lecture 7 shows that we have $ab \mid c$ if and only if $\operatorname{abs}(ab) \mid \operatorname{abs} c$. However, the same proposition shows that we have $ab \mid \operatorname{abs} c$ if and only if $\operatorname{abs}(ab) \mid \operatorname{abs}(\operatorname{abs} c)$. Since $\operatorname{abs}(\operatorname{abs} c) = \operatorname{abs} c$, the latter statement can be rewritten as $\operatorname{abs}(ab) \mid \operatorname{abs} c$. Thus, both statements $ab \mid c$ and $ab \mid \operatorname{abs} c$ are equivalent to $\operatorname{abs}(ab) \mid \operatorname{abs} c$, and thus are equivalent to each other. Hence, from $ab \mid \operatorname{abs} c$, we obtain $ab \mid c$.

Theorem 3.5.6 (coprime removal theorem)**.** Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid bc$. Assume that a is coprime to b. Then, $a \mid c$.

Proof. We have $a \mid ca$ and $a \mid bc = cb$. Thus, Corollary 3.4.9 (applied to a, ca and cb instead of m, a and b) yields

$$a \mid \gcd(ca, cb) = |c| \cdot \underbrace{\gcd(a, b)}_{\substack{=1 \\ \text{(since } a \text{ is coprime to } b\text{)}}} \qquad \text{(by Theorem 3.4.10)}$$
$$= |c|.$$

Since divisibility does not depend on signs, this means that $a \mid c$. Thus, Theorem 3.5.6 holds. □

Example 3.5.7. We have $6 \mid 7 \cdot 12$, but 6 is coprime to 7. Thus, Theorem 3.5.6 (applied to $a = 6$, $b = 7$ and $c = 12$) yields $6 \mid 12$ (as if you didn't know this already).

But we cannot obtain $6 \mid 7$ from $6 \mid 12 \cdot 7$, since 6 is not coprime to 12.

Again, Theorem 3.5.6 can be motivated using the "independence" view on coprimality: If a is coprime to b, then b cannot be the "reason" for the divisibility $a \mid bc$, and thus b can be removed from this divisibility. Again, this is neither a proof nor even a rigorous statement, but it makes Theorem 3.5.6 looks less surprising.

Theorem 3.5.8 (coprime product theorem)**.** Let $a, b, c \in \mathbb{Z}$. Assume that each of the numbers a and b is coprime to c. Then, ab is also coprime to c.

Proof. Let $g = \gcd(ab, c)$. Thus, we must prove that $g = 1$.

We have $g = \gcd(ab, c) \mid ab$ and $g = \gcd(ab, c) \mid c \mid ac$. Hence, Corollary 3.4.9 (applied to g, ab and ac instead of m, a and b) yields

$$g \mid \gcd(ab, ac) = |a| \cdot \underbrace{\gcd(b, c)}_{\substack{=1 \\ \text{(because } b \text{ is coprime to } c\text{)}}} \qquad \text{(by Theorem 3.4.10)}$$
$$= |a| \cdot 1 = |a|.$$

Hence, $g \mid a$ (since divisibility does not depend on signs). Combining this with $g \mid c$, we obtain $g \mid \gcd(a, c)$ (by Corollary 3.4.9, applied to g, a and c instead of m, a and b). However, $\gcd(a, c) = 1$ (since a is coprime to c), so we obtain $g \mid \gcd(a, c) = 1$.

However, g is a nonnegative integer (since any gcd is a nonnegative integer). Thus, g is a nonnegative divisor of 1 (since $g \mid 1$). Since the only nonnegative divisor of 1 is 1, we thus conclude that $g = 1$. Hence, $\gcd(ab, c) = g = 1$. This shows that ab is coprime to c, and we have proved Theorem 3.5.8. □

Example 3.5.9. Each of the numbers 3 and 4 is coprime to 5. Thus, Theorem 3.5.8 (applied to $a = 3$, $b = 4$ and $c = 5$) yields that $3 \cdot 4$ is coprime to 5.

Again, Theorem 3.5.8 can be viewed within the "independence" paradigm: If each of a and b is coprime to c, then so should be ab, because any "dependence" between ab and c should come from a or from b. Alternatively, if you think of coprimality as an analogue of orthogonality, then you can view Theorem 3.5.8 as an analogue of the fact that if two vectors $\overrightarrow{a}$ and $\overrightarrow{b}$ are both orthogonal to a given vector $\overrightarrow{c}$, then so is their sum $\overrightarrow{a} + \overrightarrow{b}$. Again, none of these metaphors should be mistaken for a proof of Theorem 3.5.8.

Theorems 3.5.4, 3.5.6 and 3.5.8 can be generalized, dropping some of the coprimality assumptions (but leading to less memorable results). Here is the generalization of Theorem 3.5.4:

Theorem 3.5.10. Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid c$ and $b \mid c$. Then, $ab \mid \gcd(a,b) \cdot c$.

Proof. Read our above proof of Theorem 3.5.4 until the point where it shows that $ab \mid |c| \cdot \gcd(a,b)$. Now, observe that $|c|$ divides c (since $|c|$ is either c or $-c$), and thus $|c| \cdot \gcd(a,b)$ divides $c \cdot \gcd(a,b)$. Hence,

$$ab \mid |c| \cdot \gcd(a,b) \mid c \cdot \gcd(a,b) = \gcd(a,b) \cdot c.$$

This proves Theorem 3.5.10. □

Here is the generalization of Theorem 3.5.6:

Theorem 3.5.11. Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid bc$. Then, $a \mid \gcd(a,b) \cdot c$.

Proof. Read our above proof of Theorem 3.5.6 until the point where it shows that $a \mid |c| \cdot \gcd(a,b)$. Now, observe that $|c|$ divides c (since $|c|$ is either c or $-c$), and thus $|c| \cdot \gcd(a,b)$ divides $c \cdot \gcd(a,b)$. Hence,

$$a \mid |c| \cdot \gcd(a,b) \mid c \cdot \gcd(a,b) = \gcd(a,b) \cdot c.$$

This proves Theorem 3.5.11. □

3.5.3. Reducing a fraction

Here is one more property of gcds:

Theorem 3.5.12. Let a and b be two integers that are not both 0. Let $g = \gcd(a,b)$. Then, the integers $\dfrac{a}{g}$ and $\dfrac{b}{g}$ are coprime.

This theorem is important for understanding rational numbers. Indeed, a ratio $\dfrac{u}{v}$ of two integers is said to be in **reduced form** if u and v are coprime.

Now, Theorem 3.5.12 shows that if we start with a ratio $\frac{a}{b}$ of two integers, and cancel $\gcd(a,b)$ from the numerator and the denominator, then the result will be a ratio in reduced form. Hence, each rational number can be brought to a reduced form. For example, $\frac{12}{21} = \frac{12/3}{21/3} = \frac{4}{7}$.

Proof of Theorem 3.5.12. Since a and b are not both 0, we have $\gcd(a,b) \neq 0$ (since 0 cannot divide any nonzero integer). Since we know that $\gcd(a,b) \in \mathbb{N}$, we thus conclude that $\gcd(a,b) > 0$. In other words, $g > 0$ (since $g = \gcd(a,b)$). Thus, $\frac{a}{g}$ and $\frac{b}{g}$ are well-defined. Also, from $g > 0$, we obtain $|g| = g$.

Since $g = \gcd(a,b)$, we have $g \mid a$ and $g \mid b$. Hence, $\frac{a}{g}$ and $\frac{b}{g}$ are integers. Moreover,

$$\begin{aligned} g &= \gcd(a,b) = \gcd\left(g \cdot \frac{a}{g},\ g \cdot \frac{b}{g}\right) \qquad \left(\text{since } a = g \cdot \frac{a}{g} \text{ and } b = g \cdot \frac{b}{g}\right) \\ &= \underbrace{|g|}_{=g} \cdot \gcd\left(\frac{a}{g}, \frac{b}{g}\right) \qquad \left(\begin{array}{c}\text{by Theorem 3.4.10,} \\ \text{since } \frac{a}{g} \text{ and } \frac{b}{g} \text{ are integers}\end{array}\right) \\ &= g \cdot \gcd\left(\frac{a}{g}, \frac{b}{g}\right). \end{aligned}$$

Dividing this equality by g, we find

$$1 = \gcd\left(\frac{a}{g}, \frac{b}{g}\right) \qquad (\text{since } g \neq 0).$$

This shows that $\frac{a}{g}$ and $\frac{b}{g}$ are coprime. Thus, Theorem 3.5.12 is proven. □

3.6. Prime numbers

3.6.1. Definition

The following is one of the most famous concepts in mathematics:

Definition 3.6.1. An integer $n > 1$ is said to be **prime** (or **a prime**) if the only positive divisors of n are 1 and n.

The first few primes (= prime numbers) are

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43.$$

It can be shown that there are infinitely many primes (see Exercise 4 **(b)** on homework set #4 for one proof).

3.6.2. The friend-or-foe lemma

The first property of primes that we will show is an important result that we call the **friend-or-foe lemma**:

Lemma 3.6.2 (friend-or-foe lemma)**.** Let p be a prime. Let $n \in \mathbb{Z}$. Then, n is either divisible by p or coprime to p, but not both.

Proof. The number p is prime, and thus its only positive divisors are 1 and p. Since $\gcd(n,p)$ is a positive divisor of p (this is easy to see[4]), we thus conclude that $\gcd(n,p)$ must be either 1 or p. So we are in one of the following two cases:

Case 1: We have $\gcd(n,p) = 1$.

Case 2: We have $\gcd(n,p) = p$.

Let us first consider Case 1. In this case, we have $\gcd(n,p) = 1$. In other words, n is coprime to p. Furthermore, the greatest common divisor of n and p is $\gcd(n,p) = 1$; therefore, p cannot be a common divisor of n and p (since $p > 1$). Thus, n is not divisible by p (since this would entail that p is a common divisor of n and p). So we have shown that n is coprime to p and not divisible by p. Thus, Lemma 3.6.2 is proved in Case 1.

Let us now consider Case 2. In this case, we have $\gcd(n,p) = p \neq 1$. Thus, n is not coprime to p. Also, $p = \gcd(n,p) \mid n$ shows that n is divisible by p. So we have shown that n is divisible by p and not coprime to p. Hence, Lemma 3.6.2 is proved in Case 2.

We have now proved Lemma 3.6.2 in both Cases 1 and 2; thus, Lemma 3.6.2 is fully proved. □

(The moniker "friend-or-foe lemma" is metaphorical: You can think of integers that are divisible by p as "friends of p", and think of integers coprime to p as "foes of p". Thus, a prime number cleanly divides the integers into its "friends" and its "foes". In contrast, the non-prime number 4 has a more "nuanced" relationship with certain integers such as 2 (since 2 is neither divisible by 4 nor coprime to 4).)

[4] *Proof.* The number $\gcd(n,p)$ is a divisor of p, and thus is nonzero (since 0 does not divide p). Furthermore, $\gcd(n,p)$ is nonnegative (since any gcd is nonnegative). Thus, $\gcd(n,p)$ is positive. Hence, $\gcd(n,p)$ is a positive divisor of p.

3.6.3. Binomial coefficients and primes

The friend-or-foe lemma has myriad applications. As a first example, recall Pascal's triangle (which we first saw in §2.4 in Lecture 5):

													$k{=}0$ ↙													
$n=0$	$\to$											1		$k{=}1$ ↙												
$n=1$	$\to$									1		1			$k{=}2$ ↙											
$n=2$	$\to$							1		2		1				$k{=}3$ ↙										
$n=3$	$\to$						1		3		3		1				$k{=}4$ ↙									
$n=4$	$\to$					1		4		6		4		1				$k{=}5$ ↙								
$n=5$	$\to$				1		5		10		10		5		1				$k{=}6$ ↙							
$n=6$	$\to$			1		6		15		20		15		6		1				$k{=}7$ ↙						
$n=7$	$\to$		1		7		21		35		35		21		7		1									
$n=8$	$\to$	1		8		28		56		70		56		28		8		1								

One property of Pascal's triangle that you might have already noticed is the following: All entries in its $n=7$ row except for the two 1's (i.e., all the binomial coefficients $\binom{7}{1}, \binom{7}{2}, \ldots, \binom{7}{6}$) are divisible by 7; all entries in the $n=5$ row except for the two 1's are divisible by 5; likewise for the $n=3$ and $n=2$ rows. The pattern here can be generalized to any prime number instead of $7, 5, 3, 2$:

Theorem 3.6.3. Let p be a prime. Let $k \in \{1, 2, \ldots, p-1\}$. Then, $p \mid \binom{p}{k}$.

Proof. Exercise 5 **(a)** on homework set #3 (applied to $n = p$) yields

$$k\binom{p}{k} = p \underbrace{\binom{p-1}{k-1}}_{\substack{\text{an integer} \\ \text{(by Theorem 2.5.11} \\ \text{in Lecture 6)}}}.$$

Thus, $p \mid k\binom{p}{k}$.

From $k \in \{1, 2, \ldots, p-1\}$, we furthermore obtain $p \nmid k$ (because if we had $p \mid k$, then Proposition 3.1.4 **(b)** in Lecture 7 would entail $|p| \leq |k|$, which would contradict $|k| = k \leq p-1 < p = |p|$). In other words, k is not divisible by p.

But the friend-or-foe lemma (Lemma 3.6.2, applied to $n = k$) says that k is either divisible by p or coprime to p. Since k is not divisible by p, we thus conclude that k must be coprime to p. In other words, p is coprime to k. Hence, from $p \mid k\binom{p}{k}$, we obtain $p \mid \binom{p}{k}$ using the coprime cancellation theorem (Theorem 3.5.6, applied to $a = p$ and $b = k$ and $c = \binom{p}{k}$). This proves Theorem 3.6.3. □

3.6.4. Fermat's little theorem

It is easy to see that every integer a satisfies $a^2 \equiv a \bmod 2$. Indeed, the difference $a^2 - a = a(a-1)$ is divisible by 2, since at least one of the two consecutive integers a and $a-1$ must be even and thus contributes a factor of 2 to the product $a(a-1)$.

Likewise, every integer a satisfies $a^3 \equiv a \bmod 3$, since the difference $a^3 - a = (a-1)a(a+1)$ is divisible by 3 (because at least one of the three consecutive integers $a-1$, a and $a+1$ must be divisible by 3).

This pattern does not persist for 4: Indeed, $a^4 \equiv a \bmod 4$ does not hold for $a = 2$. However, for 5, the pattern emerges again: Every integer a satisfies $a^5 \equiv a \bmod 5$. This is not as easy to see as the analogous claims for a^2 and a^3 (since $a^5 - a$ does not factor into linear factors any more), but still can be checked with a bit of work (there are only 5 possible values for the remainder $a\%5$, and each of these values allows us to check $a^5 \equiv a \bmod 5$ by reducing both sides modulo 5).

The pattern is lost again for 6 (the congruence $a^6 \equiv a \bmod 6$ fails for $a = 2$), but reemerges for 7.

As you may have guessed, there is a general result here:

Theorem 3.6.4 (Fermat's Little Theorem)**.** Let p be a prime. Let $a \in \mathbb{Z}$. Then,

$$a^p \equiv a \bmod p.$$

Proof. We shall induct on a. This will only cover the case $a \geq 0$, so we will have to handle the case $a < 0$ by a separate argument afterwards.

Base case: The congruence $a^p \equiv a \bmod p$ clearly holds for $a = 0$ (since $0^p = 0 \equiv 0 \bmod p$).

Induction step: Let $a \in \mathbb{N}$. Assume (as the induction hypothesis) that $a^p \equiv a \bmod p$. We must prove that $(a+1)^p \equiv a + 1 \bmod p$.

But the binomial formula (Theorem 2.6.1 in Lecture 6) yields

$$\begin{aligned}(a+1)^p &= \sum_{k=0}^{p} \binom{p}{k} a^k \underbrace{1^{p-k}}_{=1} = \sum_{k=0}^{p} \binom{p}{k} a^k \\ &= \underbrace{\binom{p}{0}}_{=1} \underbrace{a^0}_{=1} + \sum_{k=1}^{p-1} \binom{p}{k} a^k + \underbrace{\binom{p}{p}}_{=1} a^p \\ &\qquad \left(\begin{array}{c} \text{here, we have split off the addends} \\ \text{for } k=0 \text{ and for } k=p \text{ from the sum} \end{array} \right) \\ &= 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k + a^p = \sum_{k=1}^{p-1} \binom{p}{k} a^k + a^p + 1.\end{aligned}$$

In other words,

$$(a+1)^p - (a^p+1) = \sum_{k=1}^{p-1} \binom{p}{k} a^k. \tag{1}$$

However, Theorem 3.6.3 shows that each $k \in \{1,2,\ldots,p-1\}$ satisfies $p \mid \binom{p}{k} \mid \binom{p}{k} a^k$. In other words, $\binom{p}{k} a^k$ is a multiple of p for each $k \in \{1,2,\ldots,p-1\}$. Hence, $\sum_{k=1}^{p-1} \binom{p}{k} a^k$ is a sum of multiples of p, and thus itself a multiple of p. That is, we have $p \mid \sum_{k=1}^{p-1} \binom{p}{k} a^k$. In view of (1), we can rewrite this as $p \mid (a+1)^p - (a^p+1)$. In other words,

$$(a+1)^p \equiv a^p + 1 \bmod p. \tag{2}$$

However, the induction hypothesis says that $a^p \equiv a \bmod p$. Adding the obvious congruence $1 \equiv 1 \bmod p$ to this, we obtain

$$a^p + 1 \equiv a + 1 \bmod p.$$

Combining this congruence with (2), we obtain

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \bmod p,$$

which shows that $(a+1)^p \equiv a+1 \bmod p$ (by the transitivity of congruence). This completes the induction step.

Thus, Theorem 3.6.4 is proved for all $a \geq 0$. It remains to prove it for all $a < 0$ now. This can be done with a neat trick:

Let $a \in \mathbb{Z}$ satisfy $a < 0$. Then, we must prove that $a^p \equiv a \bmod p$.

But we already know that $b^p \equiv b \bmod p$ for all integers $b \geq 0$ (because we have already proved Theorem 3.6.4 for all $a \geq 0$). We can apply this to $b = a\%p$ (since the remainder $a\%p$ is ≥ 0), and thus obtain

$$(a\%p)^p \equiv a\%p \bmod p.$$

However, Proposition 3.3.11 **(a)** (applied to $n = a$ and $d = p$) shows that $a\%p \in \{0, 1, \ldots, p-1\}$ and $a\%p \equiv a \bmod p$. We can take the congruence $a\%p \equiv a \bmod p$ to the p-th power, we obtain $(a\%p)^p \equiv a^p \bmod p$ (we have here used Exercise 1 **(b)** on homework set #3). Therefore, $a^p \equiv (a\%p)^p \bmod p$. Combining all the congruences we have obtained so far, we obtain

$$a^p \equiv (a\%p)^p \equiv a\%p \equiv a \bmod p,$$

from which we can conclude that $a^p \equiv a \bmod p$ (by transitivity of congruence). Thus, we have proved Theorem 3.6.4 for $a < 0$. This completes the proof of Theorem 3.6.4. □

Fermat's Little Theorem has a bunch of applications, some of which we might see later.

One wrinkle in the pattern we have discussed above: Theorem 3.6.4 shows that every prime p satisfies $a^p \equiv a \bmod p$ for all $a \in \mathbb{Z}$. But there are some positive integers p that satisfy this even though they are not prime! The smallest such integers are 1, 561, 1105, 1729, 2465. See Carmichael numbers for more details.

3.6.5. Prime divisor separation theorem

You can think of the primes as "inseparable" positive integers: They cannot be written as products of two smaller positive integers. (Of course, 1 also has this property but does not count as a prime. In a way, 1 is inseparable because there is nothing to separate, so it doesn't count as a prime.)

One useful consequence of this "inseparability" is that if a prime p divides a product ab of two integers, then it must divide one of the two factors a and b, since (speaking heuristically) it cannot be "separated" into a part that divides a and a part that divides b. Nevermind that this is not a valid argument, the conclusion is a true fact:

Theorem 3.6.5 (prime divisor separation theorem)**.** Let p be a prime. Let $a, b \in \mathbb{Z}$ be such that $p \mid ab$. Then, $p \mid a$ or $p \mid b$.

Proof of Theorem 3.6.5. We shall prove the claim of Theorem 3.6.5 in the following equivalent form: "If $p \nmid a$, then $p \mid b$."

Assume that $p \nmid a$. We must then prove that $p \mid b$.

The friend-or-foe lemma (Lemma 3.6.2) yields that a is either divisible by p or coprime to p. Thus, a is coprime to p (since $p \nmid a$). In other words, p is coprime to a. Hence, we can use the coprime cancellation theorem (Theorem 3.5.6, applied to p, a and b instead of a, b and c) to obtain $p \mid b$ from $p \mid ab$. This is precisely what we wanted to prove. Theorem 3.6.5 is thus proved. □

Theorem 3.6.5 shows that if a prime number p divides a product ab, then it must divide a or b (or both). In contrast, a non-prime number like 4 can divide a product ab without dividing a or b. For example, $4 \mid 2 \cdot 6$ but $4 \nmid 2$ and $4 \nmid 6$.

We can extend Theorem 3.6.5 to products of several factors:

Corollary 3.6.6 (prime divisor separation theorem for k factors)**.** Let p be a prime. Let $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ be such that $p \mid a_1 a_2 \cdots a_k$. Then, $p \mid a_i$ for some $i \in \{1, 2, \ldots, k\}$.

(In words: If a prime divides a product of several integers, then it must divide at least one of the factors.)

Proof sketch. Induct on k. In the induction step, use Theorem 3.6.5. (The base case is the case $k = 0$, in which case Corollary 3.6.6 is vacuously true because $p \nmid 1$.) □

3.6.6. p-valuations

We will need the following simple lemma:

Lemma 3.6.7. Let p be a prime. Let n be a nonzero integer. Then, there exists a largest $m \in \mathbb{N}$ such that $p^m \mid n$.

Proof. The relation $p^m \mid n$ means that $\dfrac{n}{p^m} \in \mathbb{Z}$. In other words, it means that we can divide n by p at least m times without obtaining a non-integer. So the claim of Lemma 3.6.7 is saying that there is a largest number of times that we can divide n by p without obtaining a non-integer. But this is clear: Every time we divide n by p, the absolute value $|n|$ decreases (since $p > 1$), and obviously this cannot go on forever without eventually yielding a non-integer.

(See [19s, Proof of Lemma 2.13.22] for a more formal proof of Lemma 3.6.7.) □

Lemma 3.6.7 allows us to make the following definition:

Definition 3.6.8. Let p be a prime.

(a) Let n be a nonzero integer. Then, $v_p(n)$ shall denote the largest $m \in \mathbb{N}$ such that $p^m \mid n$. (This is well-defined by Lemma 3.6.7. Thus, $v_p(n)$ is the number of times that you can divide n by p without getting a non-integer.)

This number $v_p(n)$ will be called the **p-valuation** (or the **p-adic valuation**) of n.

(b) In order to have $v_p(n)$ defined for all integers n (as opposed to just for nonzero n), we also define $v_p(0)$ to be ∞ (because 0 can be divided by p an arbitrary number of times without any changes). This symbol ∞ is not an actual number, but we shall pretend that it behaves like a number at least in some regards. In particular, we will eventually add or compare it to other

numbers. In doing so, we shall follow the rules that

$$\begin{aligned} k + \infty = \infty + k = \infty & \qquad \text{for all } k \in \mathbb{Z}; \\ \infty + \infty = \infty; & \\ k < \infty \text{ and } \infty > k & \qquad \text{for all } k \in \mathbb{Z}; \\ \max\{\infty, k\} = \max\{k, \infty\} = \infty & \qquad \text{for all } k \in \mathbb{Z}; \\ \min\{\infty, k\} = \min\{k, \infty\} = k & \qquad \text{for all } k \in \mathbb{Z}. \end{aligned}$$

Thus, ∞ acts like a "mythical number that is larger than any actual number". We can keep up this charade as long as we only add and compare, but never subtract ∞ from anything (since $1 + \infty = \infty$ would turn into $1 = 0$ if you subtracted ∞).

Next time, we will learn more about p-valuations.

References

[19s] Darij Grinberg, *Introduction to Modern Algebra (UMN Spring 2019 Math 4281 notes)*, 29 June 2019.
`http://www.cip.ifi.lmu.de/~grinberg/t/19s/notes.pdf`