COURSE NOTES

MATH 437/537: PROF. DRAGOS GHIOCA

1. September 7

Definition 1.1. *Given integers a and b with $a \neq 0$, we say that a divides b (and we write $a \mid b$) if there exists an integer c such that $b = ac$. In this case, we say that a is a divisor of b and that b is a multiple of a.*

Proposition 1.2. *Given integers a, b, c, x, y and m, with a and m being nonzero, then we have the following properties:*

1. *if $a \mid b$, and $m \mid a$, then $m \mid b$.*
2. *if $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$.*
3. *$a \mid b$ if and only if $am \mid bm$.*
4. *$a \mid 0$ and $1 \mid b$.*
5. *if $a \mid b$ and also $b \in \mathbb{N}$, then $a \leq b$.*
6. *if $a \mid b$ then a divides also $|b|$ (the absolute value of b).*
7. *if $a \mid b$ and $b \mid a$, then $|a| = |b|$.*

Proof. The statements are clear; for example, in order to justify (1), we note that $m \mid a$ yield the existence of some integer n such that $a = mn$. On the other hand, $a \mid b$ yields the existence of some integer z such that $b = az$. So, $b = m \cdot (nz)$, i.e., $m \mid b$.

For property (3), we note that $a \mid b$ yields that $b = ax$ for some $x \in \mathbb{Z}$ and then $bm = am \cdot x$. Conversely, if $bm = am \cdot x$, then dividing by the nonzero m yields that $b = ax$.

As for justifying (7), note that $a \mid b$ yields the existence of some $x \in \mathbb{Z}$ such that $b = ax$, while $b \mid a$ yields the existence of some integer y such that $a = by$. Thus $a = a \cdot xy$ and so, $xy = 1$ (note that $a \neq 0$ because $a \mid b$). Therefore, $x = y = \pm 1$, as desired. □

Theorem 1.3. *(Division Algorithm) Given integers a and b with $a > 0$, then there exist unique integers q and r satisfying*

- (i) *$b = aq + r$; and*
- (ii) *$0 \leq r < a$.*

We call q the quotient and r the remainder for the division of b by a.

Proof. We let S be the set of all nonnegative integers of the form $b + am$, for $m \in \mathbb{Z}$. We note that S is nonempty since adding any large (positive) multiple of a to b would yield a nonnegative integer; for example, whenever $m > \left[\frac{-b}{a}\right]$ yields $b + am > 0$ (recall that $[z]$ represents the integer part of the real number z, i.e., the largest integer less than or equal to z). So, we may pick the least element in the set S, call it s_0. In particular, there exists some integer m_0 such that $s_0 := b + am_0$.

We claim that $r := s_0$ and $q := -m_0$ satisfy the properties (i)-(ii) above. The only nontrivial thing to prove is that $r < a$. Now, assuming that $r \geq a$, we derive a contradiction. Indeed, if $s_0 \geq a$, then

$$b + a(m_0 - 1) = s_0 - a \geq 0$$

is another nonnegative integer of the form $b+am$, which therefore must be contained in S. However, $s_0 - a < s_0$, which contradicts the minimality of $s_0 \in S$; so, indeed we must have that $r < a$, as desired.

Finally, we will show that the integers q and r satisfying conditions (i)-(ii) are unique. Indeed, if there were some other integers q' and r' satisfying the same two properties, then we would have that

$$r - r' = a(q' - q),$$

which means that a divides $r - r'$. However, since both r and r' are in the set $\{0, 1, \dots, a-1\}$, we conclude that

$$r - r' \in \{1 - a, \dots, -1, 0, 1, \dots, a - 1\}.$$

So, $0 \leq |r - r'| < a$ and $a \mid |r - r'|$; therefore, $|r - r'| = 0$ (see property (5) of Proposition 1.2), i.e. $r = r'$. Thus also $a(q' - q) = 0$ and therefore $q' = q$ (because $a > 0$), as claimed. □

Proposition 1.4. *Given integers a and b with $a > 0$, we have that $a \mid b$ if and only if the remainder of when we divide b by a equals 0.*

Proof. If q and r are the quotient and respectively the remainder for when we divide b by a, then $r = b - aq$. So, if $r = 0$, we get that $b = aq$ thus proving that $a \mid b$.

Now, if $a \mid b$, then also $a \mid (b - aq)$ and so, $a \mid r$. But then $0 \leq r < a$ and $a \mid r$, which means that r must be equal to 0 (see property (5) in Proposition 1.2). □

Definition 1.5. *For the integers a and b, not both equal to 0, we define the greatest common divisor of a and b, denoted by $\gcd(a, b)$, which is the largest common divisor of a and b.*

For example, $\gcd(4, 6) = 2$; $\gcd(-20, 150) = 10$, $\gcd(-21, 0) = 21$. More generally, we have the following easy properties.

Proposition 1.6. *If $a, b \in \mathbb{Z}$, not both equal to 0, then*

$$\gcd(a, b) = \gcd(b, a) = \gcd(\pm a, \pm b).$$

Also, if a is a nonzero integer, then $\gcd(a, 0) = |a|$.

Proof. This is a consequence of the fact that c and $-c$ have the same set of divisors for any integer c (see also property (6) in Proposition 1.2). □

Proposition 1.7. *If $a, b \in \mathbb{Z}$ with $a > 0$, then $a = \gcd(a, b)$ if and only if $a \mid b$.*

Proof. If $a \mid b$, then a is a common divisor of both a and b and it is the largest such commn divisor (because any divisor of a cannot be larger than a); so, $a = \gcd(a, b)$.

Now, if $a = \gcd(a, b)$, then we must also have that $a \mid b$, as claimed. □

2. September 12

The next proposition is key for us.

Proposition 2.1. *Let a and b be integers, not both equal to 0. Then $\gcd(a,b)$ is the smallest positive integer which can be written as $ax+by$ for some integers x and y.*

Proof. We let S be the set of all positive integers of the form $ax+by$ for $x,y\in\mathbb{Z}$. We note that S is nonempty since $a^2+b^2\in S$ (also, at least one of the two numbers a or b is nonzero). So, S is a nonempty set of positive integers; therefore, there exists a least element $s_0\in S$. In particular, there exist integers x_0 and y_0 such that $s_0=ax_0+by_0$.

Next we will prove that $s_0=\gcd(a,b)$. We will achieve our goal by proving the following two properties of s_0:

(1) $s_0\mid a$ and $s_0\mid b$; and
(2) s_0 is the largest among the common divisors of a and b.

Now, in order to prove (1), we prove that $s_0\mid a$ and a similar argment (reversing the role of a by b) would prove that $s_0\mid b$. So, we divide a by s_0 and obtain quotient q and remainder r. We have that

$$r=a-qs_0=a-q(ax_0+by_0)=a\cdot(1-qx_0)+b\cdot(-qy_0).$$

Thus r is a linear combination of a and b with integer coefficients; if r were positive, then it would have to be contained in the set S. On the other hand, we know that $r<s_0$ (by the Division Algorithm), so the minimality of s_0 (as an element of S) yields that $r\notin S$. So, because $r\notin S$, then r could not have been positive; so, $r=0$, which means that s_0 divides a, as desired. As mentioned before, a similar argument shows that s_0 divides also b, which finish our proof of property (1) above.

Now, in order to prove property (2) above, we note that any common divisor d of both a and b would be also a divisor for ax_0+by_0 (see property (2) of Proposition 1.2); so, $d\mid s_0$. Therefore, $d\le s_0$, which proves that s_0 is the greatest common divisor of a and b, and concludes our proof of Proposition 2.1. □

Corollary 2.2. *Let a and b be integers, not both equal to 0. Then any common divisor d of both a and b must divide also $\gcd(a,b)$.*

Proof. This is an immediate consequence of Proposition 2.1 since there must exist integers x and y such that

$$\gcd(a,b)=ax+by.$$

So, a divisor d for a and b is also a divisor for $ax+by=\gcd(a,b)$. □

Proposition 2.3. *If $d=\gcd(a,b)$ and $m\in\mathbb{N}$, then $dm=\gcd(am,bm)$.*

Proof. By Proposition 2.1, we know that d is the least positive linear combination of a and b with integer coefficients, i.e., d is the least positive integer of the form $ax+by$ with $x,y\in\mathbb{Z}$. But then dm is the least positive integer of the form $amx+bmy$ with $x,y\in\mathbb{Z}$ since we simply multiplied by m each element in the above set of linear combinations of a and b. However, again by Proposition 2.1, the least positive integer of the form $amx+bmy$ is the greatest common divisor of am and bm; so, in conclusion, $dm=\gcd(am,bm)$. □

Definition 2.4. *We say that the integers a and b are coprime if $\gcd(a,b)=1$.*

Proposition 2.5. *Let a, b and c be integers such that $a \mid bc$. If $\gcd(a,b)=1$, then $a \mid c$.*

Proof. Since $\gcd(a,b)=1$, then 1 can be written as a linear combination of a and b with integer coefficients, i.e., there exist $x,y\in\mathbb{Z}$ such that

$$1 = ax+by. \tag{1}$$

We multiply (1) by c and get

$$c = a\cdot cx + bc\cdot y. \tag{2}$$

Since $a \mid bc$, we get that $a \mid bcy$ and therefore, because also $a \mid a\cdot cx$, we conclude that $a\mid c$, as desired. □

Proposition 2.6. *Let a and b be nonzero integers. Then for any $q\in\mathbb{Z}$, we have*

$$\gcd(a,b)=\gcd(a,b+aq).$$

Proof. We can see this in two ways. On one hand, any common divisor d of a and b must also divide $b+aq$ (and a); similarly, any divisor d of a and of $b+aq$ must also divide $b=(b+aq)-a\cdot q$. So, indeed, any commn divisor of a and b is also a common divisor of a and $b+aq$, hence the equality between the two greatest common divisors.

On the other hand, $\gcd(a,b)$ is the least positive integer of the form $ax+by$ for $x,y\in\mathbb{Z}$. Also, $\gcd(a,b+aq)$ is the least positive integer of the form $az+(b+aq)t=a(z+qt)+b\cdot t$. So, each linear combination of a and $b+aq$ is also a linear combination of a and b, which proves that (by Proposition 2.1) $\gcd(a,b)\le\gcd(a,b+aq)$. Similarly, since $b=(b+aq)+a\cdot(-q)$, the exact same argument with the roles of b and $b+aq$ inversed yields that $\gcd(a,b+aq)\le\gcd(a,b)$; so, we must have that $\gcd(a,b)=\gcd(a,b+aq)$. □

2.1. Euclidean Algorithm.

Let $a,b\in\mathbb{N}$. We can find $\gcd(a,b)$ through a series of repeated subtractions, or more precisely, repeated applications of the Division Algorithm.

So, without loss of generality, we assume $a\le b$; otherwise we could switch a with b. We divide b by a and get quotient q_1 and remainder r_1:

$$b=aq_1+r_1,$$

where $0\le r_1<a$. If $r_1=0$, then we have $a\mid b$ and so, $\gcd(a,b)=a$. If $r_1>0$, then we note that

$$\gcd(a,b)=\gcd(a,r_1+aq)=\gcd(a,r_1),$$

where the last equality comes from Proposition 2.6. The advantage is that we replaced the pair $a<b$ with a "smaller" pair $r_1<a$. Then we repeat the above procedure, i.e., divide a by r_1 with quotient q_2 and remainder r_2. Once again, we get $\gcd(a,r_1)=\gcd(r_1,r_2)$; if $r_2=0$, then $\gcd(r_1,r_2)=r_1=\gcd(a,b)$, while if $r_2>0$, then the above procedure goes on. At one moment, this process needs to end since each time we decreased the positive integers we consider. So, the greatest common divisor of a and b is the last positive remainder r_n in the Euclidean Algorithm.

In particular, this process would also generate the linear combination which yields the greatest common divisor written in terms of the original numbers. We illustrate this process through an example with $a=42$ and $b=110$. So,

$$110=42\cdot 2+26;$$

thus $q_1 = 2$ and $r_1 = 26$. Then we write

$$42 = 26 \cdot 1 + 16;$$

so, $q_2 = 1$ and $r_2 = 16$. Then we write

$$26 = 16 \cdot 1 + 10,$$

which means that $q_3 = 1$ and $r_3 = 10$. Then we write

$$16 = 10 \cdot 1 + 6,$$

i.e., $q_4 = 1$ and $r_4 = 6$. Then we write

$$10 = 6 \cdot 1 + 4$$

and so, $q_5 = 1$ and $r_5 = 4$. Then we write

$$6 = 4 \cdot 1 + 2$$

and so, $q_6 = 1$ and $r_6 = 2$, which finally means that

$$4 = 2 \cdot 2 + 0,$$

i.e., $r_7 = 0$ (and $q_7 = 2$), which means that $\gcd(110, 42) = 2$ ($= r_6$, which is the last positve remainder in our Euclidean algorithm).

So, we have that

$$2 = 6 - 4 \cdot 1$$

and then substituting $4 = 10 - 6 \cdot 1$, we get

$$2 = 6 - (10 - 6 \cdot 1) \cdot 1 = 6 \cdot 2 - 10 \cdot 1.$$

We write $6 = 16 - 10 \cdot 1$ and then again substituting in the above formula, we get

$$2 = (16 - 10 \cdot 1) \cdot 2 - 10 \cdot 1 = 16 \cdot 2 - 10 \cdot 3.$$

Then using that $10 = 26 - 16 \cdot 1$, we have

$$2 = 16 \cdot 2 - (26 - 16 \cdot 1) \cdot 3 = 16 \cdot 5 - 26 \cdot 3.$$

We continue with $16 = 42 - 26 \cdot 1$ and get

$$2 = (42 - 26 \cdot 1) \cdot 5 - 26 \cdot 3 = 42 \cdot 5 - 26 \cdot 8.$$

Finally, we have that $26 = 110 - 42 \cdot 2$ and substituting this into the last equation yields 2 as a linear combination of 42 and 110:

$$2 = 42 \cdot 5 - (110 - 42 \cdot 2) \cdot 8 = 42 \cdot 21 - 110 \cdot 8.$$

3. September 14

Definition 3.1. *Let $a_1, \ldots, a_n$ be integers, not all equal to 0. We define the greatest common divisor of $a_1, \ldots, a_n$, denoted by $\gcd(a_1, \ldots, a_n)$ be the largest common divisor to all of the numbers $a_1, \ldots, a_n$.*

Arguing identically as in the proof of Proposition 2.1, we can prove the following result.

Proposition 3.2. *Let $a_1, \ldots, a_n$ be integers, not all equal to 0. Then $\gcd(a_1, \ldots, a_n)$ is the smallest positive integer which can be written as a linear combination of the numbers $a_1, \ldots, a_n$ with integer coefficients, i.e., the smallest positive integer of the form $\sum_{i=1}^{n} a_i x_i$ with $x_i \in \mathbb{Z}$ for each $i = 1, \ldots, n$.*

An immediate corollary of Proposition 3.2 is the following result.

Corollary 3.3. *Let $a_1, \dots, a_n$ be integers, not all equal to 0. Then each common divisor of the numbers $a_1, \dots, a_n$ must also divide $\gcd(a_1, \dots, a_n)$.*

Also, for each positive integer m, we have that

$$\gcd(ma_1, \dots, ma_n) = m \cdot \gcd(a_1, \dots, a_n).$$

Definition 3.4. *Let a and b be nonzero integers. We define the least common multiple of a and b, denoted $\operatorname{lcm}[a, b]$ be the smallest positive integer which is a multiple both of a and of b.*

For example, we have $\operatorname{lcm}[24, 30] = 120$ and $\operatorname{lcm}[-15, 21] = 105$. It is immediate to get the following property:

Proposition 3.5. *For any nonzero integers a and b, we have*

$$\operatorname{lcm}[a, b] = \operatorname{lcm}[b, a] = \operatorname{lcm}[\pm a, \pm b].$$

Proposition 3.6. *Let a and b be nonzero integers. Then each common multiple of a and b must be also a multiple of $\operatorname{lcm}[a, b]$.*

Proof. We let $m := \operatorname{lcm}[a, b]$ and M be a common multiple of a and b. We divide M by m with quotient q and remainder r. Since

$$r = M - qm$$

and both a and b divide both m and M, then we get that both a and b must divide also r. So, r is a common multiple of both a and b and if r is positive, then r should be at least equal to $m = \operatorname{lcm}[a, b]$, which contradicts the Division Algorithm that gives $r < m$. So, r must equal 0, which means $m \mid M$, as desired. □

Proposition 3.7. *If a and b are nonzero integers and $m \in \mathbb{N}$, then $\operatorname{lcm}[am, bm] = m \cdot \operatorname{lcm}[a, b]$.*

Proof. We let $M := \operatorname{lcm}[a, b]$ and $M_1 := \operatorname{lcm}[am, bm]$. We'll prove that $mM \mid M_1$ and also that $M_1 \mid mM$, which combined with the fact that $m, M, M_1 \in \mathbb{N}$ would yield that $M_1 = mM$ (by property (7) in Proposition 1.2).

Indeed, note that $a \mid M$ and $b \mid M$, which means that $am \mid m \cdot M$ and also $bm \mid m \cdot M$. So, mM is a common multiple of both am and bm, which means that (by Proposition 3.6), we must have that

$$M_1 \mid mM. \tag{3}$$

On the other hand, since M_1 is a multiple of am, it is also a multiple of m and therefore, $M_1 = m \cdot x$. But then $m \cdot a$ divides $M_1 = m \cdot x$ only if $a \mid x$ (see property (3) in Proposition 1.2). Similary, we get $b \mid x$ and so, x is a common multiple of both a and b. By Proposition 3.6, we get that $\operatorname{lcm}[a, b] = M$ divides x; thus $m \cdot M$ divides $m \cdot x = M_1$. In conclusion, $mM \mid M_1$ and therefore, combining this divisibility with divisibility (3), we conclude that indeed $M_1 = mM$, as claimed. □

Proposition 3.8. *Let $a, b \in \mathbb{N}$. Then $\gcd(a, b) \cdot \operatorname{lcm}[a, b] = a \cdot b$.*

Proof. We let $d = \gcd(a, b)$ and $M = \operatorname{lcm}[a, b]$. Then by Proposition 3.7, we have that

$$dM = d \cdot \operatorname{lcm}[a, b] = \operatorname{lcm}[da, db]. \tag{4}$$

On the other hand, $d \mid b$ yields that $da \mid ab$ and similarly, from $d \mid a$ we get $db \mid ab$. Thus ab is a common multiple of da and db; so, dM must divide ab (by Proposition 3.6 since dM is the least common multiple of da and db). Hence

$$dM \mid ab. \tag{5}$$

On the other hand, we have

$$dM = M \cdot \gcd(a, b) = \gcd(aM, bM), \tag{6}$$

by Proposition 2.3. Because $b \mid M$, then $ab \mid aM$; similarly, using that $a \mid M$, we get that $ab \mid bM$. So, ab is a common divisor of aM and bM; therefore, by Corollary 2.2, we get that ab must divide $\gcd(aM, bM) = dM$. Combining this divisibility with (5), we conclude that $ab = dM$ (also note that $a, b, d, M \in \mathbb{N}$ and property (7) in Property 1.2). □

Definition 3.9. *Let $a_1, \dots, a_n$ be nonzero integers. We define the least common multiple of $a_1, \dots, a_n$ (denoted $\mathrm{lcm}[a_1, \dots, a_n]$) as the smallest positive common multiple for the numbers $a_1, \dots, a_n$.*

Arguing identically as in the proof of Propositions 3.6 and 3.7, we obtain:

Proposition 3.10. *Let $a_1, \dots, a_n$ be nonzero integers. Then $\mathrm{lcm}[a_1, \dots, a_n]$ divides each common multiple of $a_1, \dots, a_n$.*

Also, if $m \in \mathbb{N}$, we have that $\mathrm{lcm}[ma_1, \dots, ma_n] = m \cdot \mathrm{lcm}[a_1, \dots, a_n]$.

4. September 19

Definition 4.1. *A prime number p is an integer greater than 1 whose positive divisors are only 1 and p.*

For example, 2, 3, 5, 7, 11 are primes. On the other hand, 6 or 15 are not primes; they are *composite* numbers (i.e., an integer greater than 1 which is *not* a prime). **Important** to note is that 1 is neither prime nor composite.

Proposition 4.2. *Each integer n greater than 1 is divisible by a prime number.*

Proof. We proceed by induction on n; the statement is clearly true for $n = 2$. Now, assuming we proved the desired conclusion whenever $n \in \{2, \dots, N-1\}$ (for some integer $N > 2$), then we prove it next when $n = N$.

Now, if N is prime, then we're done (since $N \mid N$). Otherwise, assume N is not prime and so, it must have a divisor $d \in \{2, \dots, N-1\}$. But then our inductive hypothesis yields the existence of some prime number p dividing d and thus dividing N, as claimed. □

Theorem 4.3. *There exist infinitely many prime numbers.*

Proof. Assume there exist only finitely many prime numbers; then we can list them all in a set $S = \{p_1, \dots, p_m\}$ (we know the set S is nonempty since S contains $2, 3, \dots$). We construct the number $N := 1 + \prod_{i=1}^m p_i$. Then $N > 1$ and by Proposition 4.2, we get some prime p dividing N. However, the prime p cannot be one of the primes p_j since

$$p_j \mid N = 1 + \prod_{i=1}^{m} \text{ and } p_j \mid \prod_{i=1}^{m} p_i$$

would yield that $p_j \mid 1$, contradiction. But then this means the set S does not contain *all* the possible prime numbers; therefore, there exist infinitely many prime numbers. □

Proposition 4.4. *Let p be a prime number and let $a \in \mathbb{Z}$. Then*

- *either $p \mid a$ in which case $\gcd(a, p) = p$;*
- *or $p \not| a$ in which case $\gcd(a, p) = 1$.*

Proof. If $p \mid a$, then $\gcd(a, p) = p$ (by Proposition 1.7). On the other hand, if $p \not| a$, then p and a can only share the positive common divisor 1, i.e., $\gcd(a, p) = 1$. □

Proposition 4.5. *Let p be a prime number and let $a, b \in \mathbb{Z}$. If $p \mid ab$ then either $p \mid a$ or $p \mid b$.*

Proof. Assume $p \not| a$; we'll prove that $p \mid b$. Since $p \not| a$, then Proposition 4.4 yields that $\gcd(p, a) = 1$. But then combining this condition with $p \mid ab$ along with Proposition 2.5, we obtain that $p \mid b$, as desired. □

Corollary 4.6. *Let p be a prime number and let $a_1, \dots, a_n \in \mathbb{Z}$. If $p \mid \prod_{i=1}^n a_i$, then there exists $i \in \{1, \dots, n\}$ such that $p \mid a_i$.*

Proof. We argue by induction on n; the case $n = 2$ is covered by Proposition 4.5. Now, assume the statement holds for $n = N$ and we prove it for $n = N + 1$ (for some $N \geq 2$). So, we know that

$$p \mid \prod_{i=1}^{N+1} a_i = (a_1 a_2) \cdot a_3 \cdot a_4 \cdots a_{N+1}.$$

By the inductive hypothesis, either $p \mid a_j$ for some $j = 3, \dots, N + 1$, or $p \mid a_1 a_2$. But then another application of Proposition 4.5 yields that $p \mid a_1$ or $p \mid a_2$, as claimed. □

Theorem 4.7. *(Fundamental theorem of Arithmetic) Each integer greater than 1 is written uniquely as a product of prime numbers.*

The uniqueness referred to in Theorem 4.7 doesn't refer to switching around the prime factors in the decomposition of an integer in a product of primes. So, 20 is written as $2^2 \cdot 5$ and this prime factor decomposition is unique (modulo permutations of the factors), i.e,

$$20 = 2^2 \cdot 5 = 2 \cdot 5 \cdot 2 = 5 \cdot 2 \cdot 2.$$

Proof of Theorem 4.7. First we prove that each integer n greater than 1 can be written as a product or prime numbers. Indeed, we prove this statement by induction on n; the case $n = 2$ being clear. So, we assume that all integers in the set $\{2, \dots, N - 1\}$ (for some $N > 2$) can be written as a product of primes and next we show that also N can be written as a product of primes. Indeed, if N is prime, then we're done. Now, if N is not a prime, then it must have some divisor $d \in \{2, \dots, N - 1\}$; in particular, this means that also $\ell := \frac{N}{d}$ is an integer and furthermore, it has to be in the set $\{2, \dots, N - 1\}$ (since $1 < d < N$). So, $N = d \cdot \ell$ and the inductive hypothesis gives that both d and ℓ are products of primes and therefore, $N = d \cdot \ell$ is a product of primes.

Next we will prove that modulo permutation of the prime factors, the prime factorization of any integer $n > 1$ is unique. Now, assume the contrary and therefore, assume we can write the number n in two distinct ways as a product of prime numbers, i.e.,

$$n = p_1 \cdots p_k = q_1 \cdots q_m \tag{7}$$

(where the primes p_j's and q_i's are not necessarily all distinct). Furthermore, we assume the overall number of primes $(k + m)$ appearing in (7) is minimal among all the possible representations of a positive integer as a product of primes in two distinct ways.

Since $p_1 \mid q_1 \cdots q_m$, using Corollary 4.6 yields that $p_1 \mid q_i$ for some $i = 1, \ldots, m$. On the other hand, both p_1 and q_i are prime numbers, so the only way for $p_1 \mid q_i$ is when $p_1 = q_i$. But then

$$\frac{n}{p_1} = p_2 \cdots p_k = q_1 \cdots q_{i-1} \cdot q_{i+1} \cdots q_m. \tag{8}$$

So, (8) yields a prime factorization of the integer $\frac{n}{p_1}$ in two distinct ways as a product of primes (since (7) was already a prime factorization of a number in two distinct ways). Furthermore, the total number of primes appearing in the prime factorizations from (8) is smaller than $k+m$, which we assumed to represent already the smallest possible number of primes appearing in two distinct prime factorizations of the same positive integer, contradiction. Therefore, there cannot be two distinct prime factorizations for the same positive integer.

This concludes our proof of Theorem 4.7. □

The Fundamental Theorem of Arithmetic allows us to write always any integer $n > 1$ as a product of primes, i.e,

$$n = \prod_{i=1}^{\ell} p_i^{\alpha_i}$$

for some positive integers α_i, where the primes p_i are assumed to be distinct. Also, this means that any positive divisor the number n above would be of the form

$$\prod_{i=1}^{\ell} p_i^{\beta_i},$$

for some *nonnegative* integers $\beta_i \leq \alpha_i$.

In particular, the prime factorization of integers allows us to determine easily the greatest common divisor and the least common multiple. So, if

$$m = \prod_{i=1}^{r} p_i^{\alpha_i} \text{ and } n = \prod_{i=1}^{r} p_i^{\beta_i},$$

where $\alpha_i, \beta_i \geq 0$ (note that there is no reason for m and n be divisible by the same set of distinct primes p_i, hence the assumption about the exponents α_i, β_i being nonnegative, rather than positive), then

$$\gcd(m, n) = \prod_{i=1}^{r} p_i^{\min\{\alpha_i, \beta_i\}} \text{ and } \operatorname{lcm}[m, n] = \prod_{i=1}^{r} p_i^{\max\{\alpha_i, \beta_i\}}.$$

In particular, this allows us to see immediately that

$$m \cdot n = \gcd(m, n) \cdot \operatorname{lcm}[m, n]$$

because for each $i = 1, \dots, r$, we have

$$\alpha_i + \beta_i = \min\{\alpha_i, \beta_i\} + \max\{\alpha_i, \beta_i\}.$$

5. September 21

Definition 5.1. *Let $a, b, m \in \mathbb{Z}$ with $m \neq 0$. We say that a is congruent with b modulo m and we write $a \equiv b \pmod{m}$ if $m \mid a - b$.*

If a is not congruent with b modulo m, we write $a \not\equiv b \pmod{m}$.

For example, $11 \equiv 5 \pmod{3}$, $12 \equiv -4 \pmod{8}$ and $-2 \not\equiv 9 \pmod{7}$.

Proposition 5.2. *Let m be a nonzero integer.*

(Reflexivity) *For each $a \in \mathbb{Z}$, we have $a \equiv a \pmod{m}$.*
(Symmetry) *If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.*
(Transitivity) *If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.*

Proof. The reflexivity property is immediate since $m \mid 0$. The symmetry property is also clear since $m \mid a-b$ yields $m \mid b-a$. Finally, the transitivity property follows from the fact that $m \mid a-b$ and $m \mid b-c$ yields (after addition) that $m \mid a-c$. □

Proposition 5.2 shows that being congruent modulo m is an equivalence relation on the set of all integers. So, the equivalence classes for this relation will be called residue classes modulo m.

Now, assume $m \in \mathbb{N}$. Using the Division Algorithm, we get that each integer $n \in \mathbb{Z}$ can be written uniquely as $n = qm + r$ for some $r \in \{0, \dots, m-1\}$. So, $n \equiv r \pmod{m}$ and r is unique for any given n. Therefore, the residue classes modulo m are in bijective correspondence to the integers in the set $\{0, \dots, m-1\}$. Each residue class modulo m is of the form

$$S_i := \{i + km \colon k \in \mathbb{Z}\}$$

for $i = 0, \dots, m-1$. For any integer a, when we refer to its residue class modulo m, we write $\bar{a}$ (**yes, we will always have the moduli m understood from the context**). So, for the moduli $m = 5$, we have that

$$\bar{7} = \bar{2} = \overline{-3} = \overline{2022}.$$

When we refer to a complete set of residue classes modulo m, we freely use interchangeably $\{0, \dots, m-1\}$ and $\{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$, though we will always be careful in understanding that a number $i \in \{0, \dots, m-1\}$ is an integer (even though we could view it sometimes as representing an entire residue class modulo m), while $\bar{i}$ is a residue class (modulo m), so we cannot treat it as an integer without properly understanding whether the operations we apply to $\bar{i}$ make sense. **A lot of what we will study next about congruences will allow us to give proper meaning to various operations with residue classes modulo m.**

Now, assuming m is an odd integer greater than 1 (say, $m = 2k + 1$ for some $k \in \mathbb{N}$), we often use the following set of residue classes modulo m:

$$\{-k, -k+1, \dots, -1, 0, 1, \dots, k-1, k\}.$$

Proposition 5.3. *Let $a, b, m \in \mathbb{Z}$ with $m \neq 0$ such that $a \equiv b \pmod{m}$.*

1. *If $d \mid m$, then also $a \equiv b \pmod{d}$.*
2. *If d is any integer, then also $da \equiv db \pmod{m}$.*
3. *If d is any nonzero integer, then also $da \equiv db \pmod{dm}$.*

Proof. Property (1) follows because $d \mid m$ and $m \mid (a-b)$. Property (2) follows because $m \mid (a-b)$ and so, $m \mid d(a-b)$. Finally, $m \mid (a-b)$ also yields $dm \mid d(a-b)$. □

Proposition 5.4. *If* $a \equiv b \pmod m$ *and* $c \equiv d \pmod m$ *then*

(i) $a+c \equiv b+d \pmod m$*; and*
(ii) $ac \equiv bd \pmod m$*.*

Proof. Property (i) is simple since $m \mid (a-b)$ and $m \mid (c-d)$ yields (after addition) that $m \mid (a+c)-(b+d)$. Property (ii) is more difficult since in order to prove it we need to express

$$a-b = mx \text{ for some integer } x\text{, and}$$

$$c-d = my \text{ for some integer } y.$$

Then

$$ac = (b+mx)\cdot(d+my) = bd + m\cdot(dx+by+mxy),$$

thus proving that $ac \equiv bd \pmod m$, as claimed. □

Proposition 5.4 yields that we are allowed to add, subtract and multiply congruence classes **modulo the same integer** m just the same way we would add, subtract and multiply integers, i.e.,

$$\bar{a}+\bar{b} = \overline{a+b}$$

$$\bar{a}-\bar{b} = \overline{a-b}$$

$$\bar{a}\cdot\bar{b} = \overline{a\cdot b}.$$

So, working modulo 7, we have that

$$\overline{15}+\bar{6} = \overline{21} = \bar{0}$$

$$\bar{3}-\bar{9} = \overline{-6} = \bar{1}$$

$$\bar{2}\cdot\overline{20} = \overline{40} = \bar{5}.$$

On the other hand, there is no formal division of residue classes modulo m**.** First of all, if we were to divide $\bar{3}$ by $\bar{4}$ (again modulo 7), we cannot expect to get $\overline{\frac{3}{4}}$ since we **never** defined congruence classes for rational numbers. But even if we could make the formal division of integers representing the residue classes modulo m, sometimes the answer wouldn't be unique; we'll illustrate this phenomenon next.

So, consider $m = 6$ and the residue classes (modulo 6) of $\bar{4}$ and $\bar{2}$. Then we could be tempted to write that the *division* of $\bar{4}$ by $\bar{2}$ is the residue class $\bar{2}$; however this would be wrong. First of all, the division would be a residue class $\bar{i}$ with the property that

$$\bar{2}\cdot\bar{i} = \bar{4},$$

i.e., $2i \equiv 4 \pmod 6$. However, it's not only 2 (and the entire residue class of 2 modulo 6) which solves this congruence equation but also $i = 5$ (and the entire residue class of 5 modulo 6) also satisfies the congruence equation $2i \equiv 4 \pmod 6$. This is the reason we have to be very careful not to take division of residue classes just the same way as we would divide integers. Another reason for this is the following observation, also made for the congruence classes modulo 6:

$$\bar{2}\cdot\bar{3} = \bar{0},$$

which means that the product of two residue classes may equal the residue class of 0 even though neither one of the two residue classes is the residue class of 0; this principle is opposite to the intuition you would have from multiplying integers, say.

Furthermore, the above phenomenon has the effect that only certain residue classes admit an inverse for the multiplication of residue classes. Indeed, modulo 10, you have that

$$\bar{3}\cdot\bar{7}=\bar{1},$$

i.e., the residue class $\bar{3}$ is *invertible* (see also Definition 6.1) modulo 10; however, there is no residue class $\bar{i}$ with the property that modulo 10:

$$\bar{2}\cdot\bar{i}=\bar{1},$$

since this equality of residue classes would force the congruence equation

$$2i\equiv 1 \pmod{10}$$

which implies that $2i\equiv 1 \pmod 2$ (see property (1) in Proposition 5.3), contradiction. So, even though there are quite a few similarities for the arithmetic operations for residue classes modulo the same integer m with the corresponding arithmetic operations with integers, certain differences are in place and they cannot be avoided.

6. September 26

Definition 6.1. *Let $a,m\in\mathbb{Z}$ with $m\neq 0$. We say that a is invertible modulo m, or that the residue class $\bar{a}$ of a modulo m is invertible if there exists some integer b such that $ab\equiv 1 \pmod m$, or equivalently $\bar{a}\cdot\bar{b}=\bar{1}$.*

We call the integer b an inverse for a modulo m; we call the residue class $\bar{b}$ the inverse of $\bar{a}$ modulo m.

For example, 5 is invertible modulo 7 since $5\cdot 3\equiv 1 \pmod 7$ (or $\bar{5}\cdot\bar{3}=\bar{1}$ for residue classes modulo 7). Clearly, 0 is not invertible modulo any integer $m\neq 0$; but also, as we previously observed, modulo *composite* numbers, there are also nonzero residue classes which are not invertible (for example, $\bar{2}$, $\bar{3}$ and $\bar{4}$ are not invertible modulo 6).

Proposition 6.2. *Let $a,m\in\mathbb{Z}$ with $m\neq 0$. Then a is invertible modulo m if and only if* $\gcd(a,m)=1$.

Proof. First of all, if $\gcd(a,m)=1$ then Proposition 2.1 yields that there exist integers b and x such that

$$1=ab+mx,$$

i.e., $ab\equiv 1 \pmod m$, thus proving that a is invertible modulo m.

Now, conversely, if a is invertible modulo m, then there exists some $b\in\mathbb{Z}$ such that $ab\equiv 1 \pmod m$, i.e.,

$$1=ab+mx,$$

for some integer x. So, 1 is a linear combination of a and m with integer coefficients and therefore, once again applying Proposition 2.1, we conclude that $1=\gcd(a,m)$; note that there is no positive integer smaller than 1 and so, 1 is the least positive linear combination of a and m with integer coefficients, therefore $1=\gcd(a,m)$, as claimed. □

Proposition 6.3. *Let $a,m\in\mathbb{Z}$ be coprime. Then the inverse of a modulo m is unique modulo m, i.e., any integer b which is an inverse for a modulo m belongs to the same residue class modulo m.*

Proof. Let b_1 and b_2 two integers that are both inverses for a modulo m; we'll prove that b_1 and b_2 are in the same residue class modulo m, which is the desired conclusion in Proposition 6.3.

So, we have

$$ab_1 \equiv 1 \pmod{m} \text{ and } ab_2 \equiv 1 \pmod{m}$$

which means that

$$ab_1b_2 \equiv (ab_1) \cdot b_2 \equiv 1 \cdot b_2 \equiv b_2 \pmod{m}$$

but also

$$ab_1b_2 \equiv (ab_2) \cdot b_1 \equiv 1 \cdot b_1 \equiv b_1 \pmod{m}.$$

Therefore, $b_1 \equiv b_2$, as claimed. □

Corollary 6.4. *If* $\gcd(a, m) = 1$ *(i.e., a is invertible modulo m), then for any two integers x and y we have that*

$$x \equiv y \pmod{m} \text{ if and only if } ax \equiv ay \pmod{m}.$$

Proof. First of all, if $x \equiv y \pmod{m}$ then clearly $ax \equiv ay \pmod{m}$ (according to property (2) from Proposition 5.3). Now, for the converse, we note that if $ax \equiv ay \pmod{m}$, then $m \mid a(x - y)$ and since $\gcd(a, m) = 1$, then Proposition 2.5 delivers the desired conclusion. Alternatively, we could use the fact that there exists some integer b such that $ab \equiv 1 \pmod{m}$ and then multiply the congruence

$$ax \equiv ay \pmod{m}$$

by b and then noting that $ab \equiv 1 \pmod{m}$, get

$$x \equiv y \pmod{m},$$

as desired. □

7. September 28

Proposition 7.1. *Let $P \in \mathbb{Z}[x]$ be a polynomial with integer coefficients, let $a, b, m \in \mathbb{Z}$ with $m \neq 0$. If $a \equiv b \pmod{m}$ then $P(a) \equiv P(b) \pmod{m}$.*

Proof. We have that $P(x) = \sum_{i=0}^{n} c_i x^i$ for some integers c_i (where $n = \deg(P)$). Now, using that $a \equiv b \pmod{m}$ along with repeated applications of property (ii) in Proposition 5.4, we get that

$$a^i \equiv b^i \pmod{m} \tag{9}$$

for all $i \geq 0$. (For example, if $i = 0$, then (9) is simply $1 \equiv 1 \pmod{m}$, while for $i = 2$, (9) is obtained by multiplying side-by-side the congruence $a \equiv b \pmod{m}$ with itself; for any other $i > 2$, one applies repeatedly property (ii) from Proposition 5.4 to $a \equiv b \pmod{m}$, or alternatively one can use induction on i and then the inductive step is obtained by applying property (ii) from Proposition 5.4 to $a \equiv b \pmod{m}$ and $a^{i-1} \equiv b^{i-1} \pmod{m}$.)

Then we multiply each congruence equation (9) by c_i and use one more time Proposition 5.4 (this time property (i)) to add up side-by-side all the congruences $c_i a^i \equiv c_i b^i \pmod{m}$ for $i = 0, \dots, m$, in order to conclude that $P(a) \equiv P(b) \pmod{m}$, as desired. □

Proposition 7.1 shows us that when we solve a polynomial congruence equation:

$$P(x) \equiv b \pmod{m}, \tag{10}$$

the integer solutions x will form (finitely many) residue classes modulo m since if some integer a satisfies equation (10), then all integers in the same residue class with a modulo m would work for equation (10). Therefore, when we solve a polynomial congruence equation

$$P(x) \equiv 0 \pmod{m},$$

where $P \in \mathbb{Z}[x]$, we will always be interested in the *number of residue classes* for the solutions to the above congruence equation. Note that once there exists an integer solution a to the congruence equation $P(x) \equiv 0 \pmod{m}$, then any other integer of the form $a + km$ solves the congruence equation; however, for us, the entire residue class corresponding to the integer solution a counts as just one solution since it is just one residue class.

We start solving polynomial congruence equations with the simplest case, the linear case.

Proposition 7.2. *Let $a, b, m \in \mathbb{Z}$ with $m \neq 0$; let $d := \gcd(a, m)$.*

(A) *If $d \nmid b$, then the congruence equation $ax \equiv b \pmod{m}$ has no solutions.*
(B) *If $d \mid b$, then the congruence equation $ax \equiv b \pmod{m}$ has exactly d solutions.*

Proof. The part (A) is easier since if $d \nmid b$, then any integer x_0 solving the congruence equation would yield $m \mid (ax_0 - b)$ and so, because $d \mid m$, we get $d \mid (ax_0 - b)$; but then using that $d \mid a$, we would get $d \mid b$, contradiction. This proves part (A).

Now, for part (B), we let $a = da_1$, $b = db_1$ and $m = dm_1$ for integers a_1, b_1, m_1. Furthermore, for any solution x_0 to our congruence equation, we would have that

$$dm_1 \mid d(a_1x_0 - b_1). \tag{11}$$

Combining (11) with property (3) from Proposition 1.2, we obtain that congruence $ax \equiv b \pmod{m}$ is equivalent with the congruence equation

$$a_1x \equiv b_1 \pmod{m_1}. \tag{12}$$

Now, since $\gcd(a, m) = d$ and $a = da_1$ and $m = dm_1$, we get that $\gcd(a_1, m_1) = 1$. But then Proposition 6.2 yields the existence of some $c_1 \in \mathbb{Z}$ such that

$$a_1c_1 \equiv 1 \pmod{m_1}.$$

Now, the linear congruence equation (12) is equivalent with the divisibility

$$m_1 \mid (a_1x - b_1). \tag{13}$$

Because c_1 is an inverse of a_1 modulo m_1, then it is itself invertible modulo m_1 and then again by Proposition 6.2, we have that $\gcd(c_1, m_1) = 1$. But then the divisibility (13) is equivalent with the divisibility

$$m_1 \mid c_1(a_1x - b_1). \tag{14}$$

Indeed, multiplying the right hand side in the divisibility (13) by c_1 yields (14); conversely, if the divisiblity (14) holds, since $\gcd(c_1, m_1) = 1$, then Proposition 2.5 yields the divisibility (13).

Now, divisibility (14) is the same with congruence equation

$$c_1a_1x \equiv c_1b_1 \pmod{m_1}.$$

But $c_1a_1 \equiv 1 \pmod{m_1}$ and so, the congruence equation $ax \equiv b \pmod{m}$ is equivalent with the congruence equation $a_1x \equiv b_1 \pmod{m_1}$, which is equivalent with $x \equiv b_1c_1 \pmod{m_1}$. Finally, this means that the original congruence equation $ax \equiv b \pmod{m}$ has solutions all integers of the form

$$b_1c_1 + km_1 \text{ for } k \in \mathbb{Z}. \tag{15}$$

However, these integers belong to different residue classes modulo m; more precisely, there are d distinct residue classes modulo m solving the original congruence equation $ax \equiv b \pmod{m}$. Indeed, the d distinct residue classes modulo m solving our original congruence equation correspond to the integers

$$b_1c_1 + \ell m_1 \text{ for } \ell = 0, \dots, d-1. \tag{16}$$

Clearly, all solutions from (15) are in some residue class modulo m corresponding to one of the integers from (16) because $m = d \cdot m_1$; we could write k from (15) as $\ell + rd$ for $\ell \in \{0, \dots, d-1\}$ and $r \in \mathbb{Z}$ (using the Division Algorithm) and then derive the residue classes from (16). Furthemore, each integer from (16) are distinct modulo m because

$$b_1c_1 + im_1 \equiv b_1c_1 + jm_1 \pmod{m}$$

for some $0 \le i < j \le d-1$ is equivalent with $m \mid m_1(j-i)$ and because $m = dm_1$, then this last divisibility is equivalent (according to property (3) from Proposition 1.2) to $d \mid j-i$, which is impossible because $j - i \in \{1, \dots, d-1\}$.

This concludes our proof of Proposition 7.2. □

8. October 3

Theorem 8.1. *(Chinese Remainder Theorem) Let $n \in \mathbb{N}$, let $a_1, \dots, a_n \in \mathbb{Z}$, let $m_1, \dots, m_n$ be nonzero pairwise coprime integers (i.e., $\gcd(m_i, m_j) = 1$ if $i \neq j$). Then the congruence system of (linear) equations*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \cdots\cdots\cdots\cdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

has a unique solution modulo $\prod_{i=1}^n m_i$.

Proof. First of all, it is easier to see that any two solutions x and y to the given system of linear congruences must be in the same residue class modulo $M := \prod_{i=1}^n m_i$. Indeed, for each $i = 1, \dots, n$, we have that

$$x \equiv a_i \equiv y \pmod{m_i},$$

i.e., $m_i \mid x - y$ for each $i = 1, \dots, n$. So, $x - y$ must be divisible by each m_i and thus, it is divisible by $\operatorname{lcm}[m_1, \dots, m_n]$. But since $\gcd(m_i, m_j) = 1$, we have that $\operatorname{lcm}[m_1, \dots, m_n] = M$, i.e.,

$$x \equiv y \pmod{\prod_{i=1}^n m_i}.$$

Now, for the existence of a solution to our system of congruence equations, we argue as follows. For each $i = 1, \dots, n$, we let

$$M_i := \prod_{\substack{1 \le j \le n \\ j \neq i}} m_j.$$

Since $\gcd(m_i, m_j) = 1$ for $i \neq j$, then $\gcd(m_i, M_i) = 1$ for each $i = 1, \dots n$. So, M_i is invertible modulo m_i (by Proposition 6.2); thus there exists $b_i \in \mathbb{Z}$ such that

$$b_i M_i \equiv 1 \pmod{m_i}.$$

We claim that $x_0 := \sum_{i=1}^{n} a_i b_i M_i$ is a solution to the given system of congruence equations. Indeed, for each $i = 1, \dots, n$, we have that $m_i \mid M_j$ if $j \neq i$; so,

$$x_0 \equiv a_1 b_1 M_1 + \cdots + a_n b_n M_n \equiv a_i b_i M_i \equiv a_i \cdot 1 \equiv a_i \pmod{m_i}.$$

This concludes our proof of Theorem 8.1. □

Theorem 8.2. *For a polynomial $P \in \mathbb{Z}[x]$ and for any nonzero integer m, we denote by $N_P(m)$ the number of solutions to the polynomial congruence*

$$P(x) \equiv 0 \pmod{m},$$

i.e., the number of distinct residue classes modulo m corresponding to integer solutions to the above congruence equation. Then for any two coprime nonzero integers m_1 and m_2, we have that $N_P(m_1 m_2) = N_P(m_1) \cdot N_P(m_2)$.

Proof. The first observation is that for each positive integer m, the number of solutions for the polynomial congruence $P(x) \equiv 0 \pmod{m}$ is the number of integers $i \in \{0, \dots, m-1\}$ satisfying $m \mid P(i)$. We denote by $S(m)$ the subset of $\{0, \dots, m-1\}$ consisting of solutions to the congruence equation $f(x) \equiv 0 \pmod{m}$.

Now, let m_1 and m_2 be coprime positive integers. We note that for each integer $i \in \{0, \dots, m_1 m_2 - 1\}$, we have that $m_1 m_2 \mid P(i)$ if and only if $m_1 \mid P(i)$ *and* $m_2 \mid P(i)$ (since m_1 and m_2 are coprime). So, for each $i \in \{0, \dots, m_1 m_2 - 1\}$, we let $i_1 \in \{0, \dots, m_1 - 1\}$ and $i_2 \in \{0, \dots, m_2 - 1\}$ such that

$$i \equiv i_1 \pmod{m_1} \text{ and } i \equiv i_2 \pmod{m_2};$$

note that i_1 and i_2 are the remainders when we divide i by m_1, respectively by m_2. Since the remainder of an integer when divided by another positive integer is uniquely determined, we see that the function

$$f : \{0, \dots, m_1 m_2 - 1\} \longrightarrow \{0, \dots, m_1 - 1\} \times \{0, \dots, m_2 - 1\}$$

given by $i \mapsto (i_1, i_2)$ is well-defined. Furthermore, the Chinese Remainder Theorem yields that f is a bijection since for any given $a \in \{0, \dots, m_1 - 1\}$ and $b \in \{0, \dots, m_2 - 1\}$, there exists a unique $i \in \{0, \dots, m_1 m_2 - 1\}$ such that $i \equiv a \pmod{m_1}$ and $i \equiv b \pmod{m_2}$.

As previously observed, we see that $i \in \{0, \dots, m_1 m_2 - 1\}$ is a solution to $P(x) \equiv 0 \pmod{m_1 m_2}$ if and only if writing $f(i) = (i_1, i_2)$, we have that i_1 is a solution to $P(x) \equiv 0 \pmod{m_1}$ and i_2 is a solution to $P(x) \equiv 0 \pmod{m_2}$; indeed, note that

$$P(i) \equiv P(i_1) \equiv 0 \pmod{m_1} \text{ because } i \equiv i_1 \pmod{m_1}$$

and

$$P(i) \equiv P(i_2) \equiv 0 \pmod{m_2} \text{ because } i \equiv i_2 \pmod{m_2}.$$

So, this means we have a well-defined map, denoted $\bar{f}$ when we restrict f to a function

$$\bar{f} : S(m_1 m_2) \longrightarrow S(m_1) \times S(m_2)$$

given by $\bar{f}(i) = (i_1, i_2)$ as defined above for f. Furthermore, the Chinese Remainder Theorem (CRT) applied to any pair $(a, b) \in S(m_1) \times S(m_2)$, i.e., applying CRT to the system of congruence equations

$$x \equiv a \pmod{m_1} \text{ and } x \equiv b \pmod{m_2},$$

shows that there exists a unique solution $x_0 \in \{0, \dots, m_1m_2 - 1\}$. That corresponding solution x_0 must satisfy that $m_1 \mid f(x_0)$ and also $m_2 \mid f(x_0)$, which means that $m_1m_2 \mid f(x_0)$ (since $\gcd(m_1, m_2) = 1$ which means that $\operatorname{lcm}[m_1, m_2] = m_1m_2$). Thus $x_0 \in S(m_1m_2)$, i.e., for any $(a, b) \in S(m_1) \times S(m_2)$, there exists a unique $x_0 \in S(m_1, m_2)$ such that $\bar{f}(x_0) = (a, b)$. Therefore, $\bar{f}$ is a bijection, thus proving that $\#S(m_1m_2) = \#S(m_1) \cdot \#S(m_2)$, i.e., $N_P(m_1m_2) = N_P(m_1) \cdot N_p(m_2)$. □

9. October 5

Definition 9.1. *The function $f : \mathbb{N} \longrightarrow \mathbb{C}$ is called multiplicative if for each coprime $m, n \in \mathbb{N}$, we have $f(m \cdot n) = f(m) \cdot f(n)$.*

If the function $f : \mathbb{N} \longrightarrow \mathbb{C}$ satisfies the property $f(mn) = f(m) \cdot f(n)$ for every *$m, n \in \mathbb{N}$, then we call f completely multiplicative.*

As proven in Theorem 8.2, for any polynomial $P \in \mathbb{Z}[x]$, denoting by $N_P : \mathbb{N} \longrightarrow \mathbb{N} \cup \{0\}$ the function which assigns to each positive integer m the number of solutions for the polynomial congruence equation:

$$P(x) \equiv 0 \pmod{m},$$

then N_P is a multiplicative function. This means that whenever we want to determine the number of solutions for a given polynomial congruence equation $P(x) \equiv 0 \pmod{m}$, we first write the prime factorization of m:

$$m = \prod_{i=1}^{r} p_i^{\alpha_i}$$

and then we solve each polynomial congruence

$$P(x) \equiv 0 \pmod{p_i^{\alpha_i}} \text{ for } i = 1, \dots, r.$$

Then $N_P(m) = \prod_{i=1}^{r} N_P\left(p_i^{\alpha_i}\right)$.

Definition 9.2. *For each positive integer n, we denote by $d(n)$ the number of positive divisors of n.*

For example, $d(2) = 2$, $d(3) = 2$, $d(4) = 3$, $d(5) = 2$, $d(6) = 4$, and so on.

Proposition 9.3. *Let m and n be coprime positive integers. Then each positive divisor d of $m \cdot n$ can be written uniquely as a product $d_1 \cdot d_2$, where d_1 is a positive divisor of m, while d_2 is a positive divisor of n.*

Proof. Indeed, we let $d_1 := \gcd(d, m)$ and $d_2 = \gcd(d, n)$. Note that this definition for d_1 and d_2 matches the conclusion we seek since if $d = d_1 \cdot d_2$ with $d_1 \mid m$ and $d_2 \mid n$, then necessarily we have that $d_1 = \gcd(d, m)$ and $d_2 = \gcd(d, n)$ because $\gcd(m, n) = 1$. In other words, the uniqueness of d_1 and d_2 is guaranteed by our construction of d_1 and d_2; however, we have to prove the existence of such a writing of d in terms of d_1 and d_2, i.e., we need to prove that letting $d_1 = \gcd(d, m)$ and $d_2 = \gcd(d, n)$ would also guarantee that $d = d_1 \cdot d_2$.

Now, since $d_1 \mid m$ and $d_2 \mid n$, while $\gcd(m,n) = 1$, then we have that $\gcd(d_1, d_2) = 1$. Furthermore, since $d_1 \mid d$ and $d_2 \mid d$ and $\gcd(d_1, d_2) = 1$, then we must have that $d_1 d_2 \mid d$. So, there exists some $k \in \mathbb{N}$ such that $d = d_1 d_2 k$.

Now, assume $k > 1$; then there exists some prime p dividing k. Since

$$p \mid k \mid d \mid mn,$$

then $p \mid m$ or $p \mid n$. We assume that $p \mid m$ and we will derive a contradiction; a similar argument would work if we were to assume $p \mid n$. So,

$$pd_1 \mid kd_1 \mid d \mid mn$$

and also, since $p \mid m$ and $\gcd(m,n) = 1$, then $\gcd(p,n) = 1$. Along with the fact that also $\gcd(d_1, n) = 1$ because $d_1 \mid m$ and $\gcd(m,n) = 1$, then we have that $\gcd(pd_1, n) = 1$. But combining this last fact with the divisibility $pd_1 \mid mn$, then using Proposition 2.5, we conclude that

$$pd_1 \mid m.$$

So, using that also $pd_1 \mid d$, we would have that $pd_1 \mid gcd(d,m) = d_1$, contradiction. So, indeed there is no prime p dividing k, which means that k must equal 1 an so, $d = d_1 d_2$, as claimed in Proposition 9.3. □

In this lecture, when referring to positive divisors of a positive integer, we will often call them simply divisors.

Proposition 9.4. *The function $d : \mathbb{N} \longrightarrow \mathbb{N}$ is multiplicative.*

Proof. Let m and n be coprime positive integers. According to Proposition 9.3, each divisor d of $m \cdot n$ is of the form $d_1 \cdot d_2$ with $d_1 \mid m$ and $d_2 \mid n$. Conversely, it is clear that for any two divisors d_1 of m and d_2 of n, then $d := d_1 \cdot d_2$ is a divisor of $m \cdot n$. Therefore, we have a bijection between the sets

$$D(mn) \mapsto D(m) \times D(n), \tag{17}$$

where for each positive integer k, we denote by $D(k)$ the set of all positive divisors of k; the map from (17) is given by $d \mapsto (d_1, d_2)$ where $d = d_1 d_2$ and $d_1 \mid m$ while $d_2 \mid n$ as in Proposition 9.3. Equation (17) delivers the desired conclusion for Proposition 9.4. □

Proposition 9.4 allows us to compute $d(n)$ for any positive integer n. First of all, if $n = 1$, then clearly $d(1) = 1$. Now, if $n > 1$ then we write

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

and since $d : \mathbb{N} \longrightarrow \mathbb{N}$ is a multiplicative function, then

$$d(n) = \prod_{i=1}^{r} d\left(p_i^{\alpha_i}\right).$$

However, for any prime power p^α, we note that the positive divisors of p^α are the $\alpha + 1$ integers

$$1, p, p^2, \cdots, p^\alpha.$$

So, $d(p^\alpha) = \alpha + 1$ for any prime p and any nonnegative integer α. In conclusion,

$$d(n) = d\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} d\left(p_i^{\alpha_i}\right) = \prod_{i=1}^{r} (\alpha_i + 1).$$

Definition 9.5. *For each positive integer n, we define $\sigma(n)$ be the sum of all positive divisors of n.*

For example, $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 4$, $\sigma(4) = 7$, $\sigma(5) = 6$, $\sigma(6) = 12$ and so on.

Proposition 9.6. *The function $\sigma : \mathbb{N} \longrightarrow \mathbb{N}$ is multiplicative.*

Proof. Let m and n be coprime positive integers. Using Proposition 9.3, we observe that

$$\sigma(mn) = \sum_{d \mid mn} d = \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} d_1 \cdot d_2 = \left(\sum_{d_1 \mid m} d_1 \right) \cdot \left(\sum_{d_2 \mid n} d_2 \right) = \sigma(m) \cdot \sigma(n),$$

as desired in the conclusion of Proposition 9.6. □

Proposition 9.6 allows us to compute the sum of positive divisors for any positive integer

$$n = \prod_{i=1}^{r} p_i^{\alpha_i},$$

since we obtain

$$\sigma(n) = \prod_{i=1}^{r} \sigma\left(p_i^{\alpha_i}\right).$$

Then for each prime power p^α (where p is prime and α is a nonnegative integer), we have that

$$\sigma\left(p^\alpha\right) = 1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}.$$

In conclusion,

$$\sigma(n) = \sigma\left(\prod_{i=1}^{r} p_i^{\alpha_i} \right) = \prod_{i=1}^{r} \left(\frac{p_i^{\alpha_i + 1} - 1}{p_i - 1} \right).$$

Definition 9.7. *For each positive integer n, we denote by $\phi(n)$ the number of integers from the set $\{0, \ldots, n-1\}$, which are coprime with n.*

The function $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ counts the number of residue classes modulo n which contain integers coprime with n (since if $\gcd(i, n) = 1$, then $\gcd(i + kn, n) = 1$ for all $k \in \mathbb{Z}$). The function ϕ is also called the Euler-totient function.

For example, for any prime p, we have $\phi(p) = p - 1$ since - with the exception of 0 - every other integer from the set $\{0, 1, \ldots, p-1\}$ is coprime with the prime p. Furthermore, for each prime power p^α, we count the numbers in the set $\{0, 1, \ldots, p^\alpha - 1\}$ not divisible by p; those are the numbers *divisible* by p and there are $p^{\alpha-1}$ such numbers in the above set, i.e., the numbers:

$$0, p, 2p, 3p, \cdots, p^\alpha - p.$$

So, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$.

10. October 10

Proposition 10.1. *The function $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ is multiplicative.*

Proof. Let m and n be coprime positive integers.

We constructed in the proof of Theorem 8.2 the function

$$f : \{0, 1, \dots, mn-1\} \longrightarrow \{0, 1, \dots, m-1\} \times \{0, 1, \dots, n-1\}$$

given by $i \mapsto (i_1, i_2)$, where $i_1 \in \{0, \dots, m-1\}$ and $i_2 \in \{0, \dots, n-1\}$ are the corresponding remainders when we divide $i \in \{0, \dots, mn-1\}$ by m, respectively n; in the proof of Theorem 8.2, we proved that the function f is bijective.

Now, for each positive integer k, we let $S_\phi(k)$ be the set of all integers $i \in \{0, 1, \dots, k-1\}$ which are coprime with k; so, $\phi(k) = \#S_\phi(k)$. We claim that the restriction of f to $S_\phi(mn)$ induces a well-defined function

$$g : S_\phi(mn) \longrightarrow S_\phi(m) \times S_\phi(n).$$

In order to prove that g is well-defined, we need to make sure that when we restrict the function f to $S_\phi(mn)$, then its image lives inside $S_\phi(m) \times S_\phi(n)$. So, let $i \in S_\phi(mn)$; then $\gcd(i, mn) = 1$. In particular, this means that $\gcd(i, m) = 1$ and letting i_1 be the remainder of i when we divide by m, then we also get that $\gcd(i_1, m) = 1$ (indeed, note that $i = i_1 + qm$ for some integer q and therefore, since i and m share no common divisor, then also i_1 and m share no common divisor). So, indeed, the image of i under the function f produces a pair

$$(i_1, i_2) \in \{0, 1, \dots, m-1\} \times \{0, 1, \dots, n-1\}$$

for which $\gcd(i_1, m) = 1$ and $\gcd(i_2, n) = 1$, i.e., actually $i_1 \in S_\phi(m)$ and $i_2 \in S_\phi(n)$. So, the function

$$g : S_\phi(mn) \longrightarrow S_\phi(m) \times S_\phi(n)$$

is well-defined. Now, in order to prove that $\phi(mn) = \phi(m) \cdot \phi(n)$, it suffices to prove that g is a bijection (since $\phi(mn) = \#S_\phi(mn)$, $\phi(m) = \#S_\phi(m)$ and $\phi(n) = \#S_\phi(n)$). Now, we get that g is a bijection using Theorem 8.1 because for each

$$(a, b) \in S_\phi(m) \times S_\phi(n),$$

the system of congruences

$$x \equiv a \pmod{m} \text{ and } x \equiv b \pmod{n}$$

has a unique solution $x_0 \in \{0, 1, \dots, mn-1\}$. Because $a \in S_\phi(m)$ we have that $\gcd(a, m) = 1$ and since $x_0 \equiv a \pmod{m}$ then also $\gcd(x_0, m) = 1$. Similarly, since $b \in S_\phi(n)$, then $\gcd(b, n) = 1$ and because $x_0 \equiv b \pmod{n}$ then also $\gcd(x_0, n) = 1$. Combining the fact that x_0 is coprime with both m and n yields that $\gcd(x_0, mn) = 1$, i.e., $x_0 \in S_\phi(mn)$. Therefore, the Chinese Remainder Theorem guarantees the fact that the function

$$g : S_\phi(mn) \longrightarrow S_\phi(m) \times S_\phi(n)$$

is a bijection. This concludes our proof of Proposition 10.1. □

Proposition 10.1 allows us to compute the Euler-totient function for each positive integer

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}.$$

Indeed, because ϕ is a multiplicative function and

$$\phi\left(p^{\alpha}\right) = p^{\alpha} - p^{\alpha-1} = p^{\alpha-1}(p-1) = p^{\alpha} \cdot \left(1 - \frac{1}{p}\right),$$

we obtain

$$\phi(n) = \phi\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} \phi\left(p_i^{\alpha_i}\right)$$

$$\phi(n) = \prod_{i=1}^{r}\left(p_i^{\alpha_i} - p_i^{\alpha_i-1}\right) = \prod_{i=1}^{r} p_i^{\alpha_i-1}(p_i - 1) = \prod_{i=1}^{r} p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$$

The next result is one of the most important results from our course.

Theorem 10.2. *(Euler's Theorem) Let $m \in \mathbb{N}$ and let $a \in \mathbb{Z}$ be coprime with m. Then*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Since $\phi(p) = p - 1$ for any prime number p, then the following result is an immediate consequence of Theorem 10.2.

Theorem 10.3. *(Fermat's Little Theorem) Let p be a prime number and let $a \in \mathbb{Z}$ such that $p \not| a$. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Corollary 10.4. *Let p be a prime number and let $a \in \mathbb{Z}$. Then*

$$a^{p} \equiv a \pmod{p}.$$

Proof. If $p \mid a$, then clearly

$$a^{p} \equiv a \equiv 0 \pmod{p}.$$

Now, if $p \not| a$, then Theorem 10.3 yields that

$$a^{p-1} \equiv 1 \pmod{p}$$

and then multiplying the above last congruence by a yields the desired conclusion in Corollary 10.4. □

Proof of Theorem 10.2. With the notation as before, we let

$$S_{\phi}(m) = \{0 \le i \le m-1\colon \gcd(i, m) = 1\};$$

so, $\phi(m) = \# S_{\phi}(m)$. For each $i \in S_{\phi}(m)$, we let $h(i)$ be the remainder of $a \cdot i$ when we divide it by m.

Claim 10.5. *With the above notation, for each $i \in S_{\phi}(m)$ we have that $h(i) \in S_{\phi}(m)$.*

Proof of Claim 10.5. Since both i and a are coprime with m, then also ai is coprime with m and then its remainder modulo m is coprime with m (see Proposition 2.6). Since by definition, we have that $0 \le h(i) \le m-1$, then this concludes our proof of Claim 10.5. □

Using Claim 10.5, we get that the function

$$h : S_{\phi}(m) \longrightarrow S_{\phi}(m)$$

is well-defined.

Claim 10.6. *The function h is bijective.*

Proof of Claim 10.6. Since h is a function from a finite set into itself, all we need to prove is that h is injective since then it is automatically bijective. **Very important, this property about maps from a set into itself is only valid if the set is finite.**

So, let $i_1, i_2 \in S_\phi(m)$ and assume $h(i_1) = h(i_2)$. By definition of the function h, we have that $h(i_1)$ is the remainder of ai_1 when divided by m, which means that

$$h(i_1) \equiv ai_1 \pmod{m},$$

while $h(i_2)$ is the remainder of ai_2 when divided by m, which means that

$$h(i_2) \equiv ai_2 \pmod{m}.$$

In conclusion, $h(i_1) = h(i_2)$ would force

$$ai_1 \equiv ai_2 \pmod{m},$$

i.e., $m \mid (ai_1 - ai_2)$ and thus $m \mid a(i_1 - i_2)$. But since $\gcd(m, a) = 1$, then Proposition 2.5 yields $m \mid (i_1 - i_2)$. However, $i_1, i_2 \in \{0, \dots, m-1\}$, which means that the only way we could have that $m \mid i_1 - i_2$ is when $i_1 = i_2$. So, indeed, h is an injective function, and therefore it is a bijective function.

This proves our Claim 10.6. □

Since h is bijective, then we have

$$\prod_{i \in S_\phi(m)} h(i) \equiv \prod_{i \in S_\phi(m)} i \pmod{m}, \text{ i.e.} \tag{18}$$

$$\prod_{i \in S_\phi(m)} ai \equiv \prod_{i \in S_\phi(m)} i \pmod{m}. \tag{19}$$

We let $P := \prod_{i \in S_\phi(m)} i$; since each element in $S_\phi(m)$ is coprime with m, we conclude that

$$\gcd(P, m) = 1. \tag{20}$$

So, congruence (19) yields

$$m \mid a^{\phi(m)} \cdot P - P \tag{21}$$

because $\phi(m) = \#S_\phi(m)$. But then $m \mid P \cdot \left(a^{\phi(m)} - 1\right)$ and combining this divisibility with (20) along with Proposition 2.5, we obtain

$$m \mid a^{\phi(m)} - 1,$$

as desired in the conclusion of Theorem 10.2. □

11. October 12

Theorem 11.1. *(Wilson's theorem) Let p be a prime number. Then*

$$p \mid (p-1)! + 1. \tag{22}$$

Proof. Equation (22) clearly holds when $p = 2$ or $p = 3$; so, from now on, we assume $p \geq 5$.

Claim 11.2. *For each $i \in \{2, \dots, p-2\}$, there exists a unique $j \in \{2, \dots, p-2\}$, not equal with i, such that*

$$ij \equiv 1 \pmod{p}. \tag{23}$$

Proof of Claim 11.2. Equation (23) tells us that we're asked to prove that each integer in the set $\{2, \ldots, p-2\}$ admits an inverse modulo p, which is not the integer itself. Now, the fact that each integer in the set $\{2, \ldots, p-2\}$ admits an inverse is a consequence of the fact that the prime p is coprime with each such integer; also, the inverse is unique, as proved in Proposition 6.3. So, all we need to show is that the inverse of each $i \in \{2, \ldots, p-2\}$ actually lives in $\{2, \ldots, p-2\}$ and that the inverse is not i itself.

Now, the fact that the inverse of $i \in \{2, \ldots, p-2\}$ must also live in the same set is because otherwise, the inverse of i is either 1 or $p-1$ (note that 0 cannot be an inverse since it's not coprime with p). But if the inverse of i is 1, then we would have

$$i \cdot 1 \equiv i \not\equiv 1 \pmod{p},$$

(note that $2 \leq i \leq p-2$ and so, $i \not\equiv 1 \pmod{p}$), while if the inverse of i were $p-1$, then we would have

$$i \cdot (p-1) \equiv -i \not\equiv 1 \pmod{p}$$

(again note that $2 \leq i \leq p-2$ and so, $i \not\equiv p-1 \pmod{p}$). So, the inverse j of i modulo p cannot be 1 or $p-1$, which means that $j \in \{2, \ldots, p-2\}$.

Finally, we show that $j \neq i$ since otherwise we would have

$$1 \equiv i \cdot j \equiv i^2 \pmod{p},$$

i.e., $p \mid i^2 - 1$ and so, $p \mid (i-1)(i+1)$, which means that either $p \mid i-1$ or $p \mid i+1$. But this would mean that either $i \equiv 1 \pmod{p}$ or $i \equiv p-1 \pmod{p}$, both options being impossible because $i \in \{2, \ldots, p-2\}$.

This concludes our proof of Claim 11.2. □

Using Claim 11.2, we can define a function

$$f : \{2, \ldots, p-2\} \longrightarrow \{2, \ldots, p-2\}$$

such that $f(i)$ is the inverse of i modulo p. Furthermore, $f(i) \neq i$ for each $i \in \{2, \ldots, p-2\}$. This allows us to split the product of all integers $i \in \{2, \ldots, p-2\}$ in product of pairs $(i \cdot f(i))$; we would have $\frac{p-3}{2}$ such pairs. Clearly, the product of each such pair is congruent with 1 modulo p, which means that

$$\prod_{i=2}^{p-2} i \equiv 1 \pmod{p}.$$

Therefore,

$$(p-1)! \equiv (1 \cdot (p-1)) \cdot \prod_{i=2}^{p-2} i \equiv -1 \pmod{p},$$

as claimed in equation (22). □

Proposition 11.3. *Let p be a prime satisfying $p \equiv 1 \pmod{4}$. Then*

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{4}.$$

Proof. From Wilson's Theorem, we know that

$$1 \cdot 2 \cdots (p-1) \equiv -1 \pmod{p}.$$

We define a function

$$g:\left\{\frac{p+1}{2},\cdots,p-1\right\}\longrightarrow\left\{1,\dots,\frac{p-1}{2}\right\}$$

given by $g(i)=p-i$. Clearly, g is a well-defined bijective function. Furthermore, $g(i)\equiv -i\pmod{p}$, which means that

$$-1\equiv\prod_{i=1}^{p-1}i\equiv\prod_{i=1}^{\frac{p-1}{2}}\cdot\prod_{i=\frac{p+1}{2}}^{p-1}i\pmod{p}$$

and so,

$$-1\equiv\left(\frac{p-1}{2}\right)!\cdot\prod_{i=1}^{\frac{p-1}{2}}g(i)\pmod{p}$$

and therefore,

$$-1\equiv\left(\frac{p-1}{2}\right)!\cdot\prod_{i=1}^{\frac{p-1}{2}}(-i)\equiv\left(\frac{p-1}{2}\right)!\cdot(-1)^{\frac{p-1}{2}}\cdot\left(\frac{p-1}{2}\right)!\pmod{p}.$$

Finally, using that $p\equiv 1\pmod{4}$, i.e., $\frac{p-1}{2}$ is an even integer, we conclude that

$$-1\equiv\left(\left(\frac{p-1}{2}\right)!\right)^2\pmod{p},$$

as desired. □

12. October 17

In particular, Proposition 11.3 shows that for a prime p of the form $4k+1$, we have that the congruence equation

$$x^2\equiv -1\pmod{p}$$

is solvable. Next, we show that the same congruence equation has no solutions if p were of the form $4k+3$.

Proposition 12.1. *Let p be a prime satisfying $p\equiv -1\pmod{4}$. Then the quadratic congruence equation*

$$x^2\equiv -1\pmod{4}\tag{24}$$

is unsolvable.

Proof. Assume $x_0\in\mathbb{Z}$ is a solution to congruence equation (24). Since $p\mid x_0^2-1$, then $p\not| x_0^2$ and so, $\gcd(p,x_0)=1$. Therefore, by Theorem 10.3, we have that

$$x_0^{p-1}\equiv 1\pmod{p}.\tag{25}$$

However, using (24), we get

$$x_0^{p-1}\equiv\left(x_0^2\right)^{\frac{p-1}{2}}\equiv(-1)^{\frac{p-1}{2}}\equiv -1\pmod{p}\tag{26}$$

because $\frac{p-1}{2}$ is an odd integer (note that $p\equiv -1\pmod{4}$). So, congruences (25) and (26) are contradictory, thus proving that there exists no solution to the quadratic congruence equation (24). □

Corollary 12.2. *Let $p\equiv -1\pmod{4}$ be a prime number. Then for any two integers a and b, if $p\mid(a^2+b^2)$, then we must have that $p\mid a$ and $p\mid b$.*

Proof. First of all, if $p \mid a$, then since $p \mid (a^2+b^2)$, we would get that $p \mid b^2$ and therefore, $p \mid b$, as desired. So, from now on, we assume $p \not| a$.

But then there exists some integer c such that $ac \equiv 1 \pmod{p}$ and so, multiplying by c^2 the congruence relation:

$$a^2+b^2 \equiv 0 \pmod{p},$$

we get

$$0 \equiv c^2 \cdot (a^2+b^2) \equiv (ca)^2 + (cb)^2 \equiv 1 + (cb)^2 \pmod{p}.$$

But this last congruence shows that the quadratic congruence equation

$$x^2+1 \equiv 0 \pmod{p}$$

is solvable, therefore contradicting Proposition 12.1.

This concludes our proof of Corollary 12.2. □

13. October 19

Theorem 13.1. *Let p be a prime satisfying $p \equiv 1 \pmod{4}$. Then there exist $a, b \in \mathbb{N}$ such that $a^2+b^2=p$.*

Proof. We let

$$S = \{m \in \mathbb{N}\colon \text{ there exists } x, y \in \mathbb{Z} \text{ such that } mp = x^2+y^2\}.$$

Clearly, S is nonempty since $p \in S$ because $p \cdot p = p^2 + 0^2$. So, we can pick the least element $m_0 \in S$; our goal is to prove that $m_0 = 1$. In particular, we know there exist some $x_0, y_0 \in \mathbb{Z}$ such that

$$x_0^2 + y_0^2 = m_0 p.$$

First we prove the following:

Claim 13.2. *With the above notation, $m_0 < p$.*

Proof of Claim 13.2. We know (by Proposition 11.3) that there exists some $m_1 \in \mathbb{N}$ such that

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 + 1 = m_1 p. \tag{27}$$

We let $i \in \left\{-\frac{p-1}{2}, -\frac{p-3}{2}, \dots, -1, 0, 1, \dots, \frac{p-1}{2}\right\}$ such that

$$\left(\frac{p-1}{2}\right)! \equiv i \pmod{p}. \tag{28}$$

Combining (27) and (28), we get that there exists some $m_2 \in \mathbb{N}$ such that

$$i^2 + 1 = m_2 p. \tag{29}$$

Equation (29) yields that $m_2 \in S$ and since m_0 is the least element of S, then we have that $m_0 \le m_2$. On the other hand, because $|i| \le \frac{p-1}{2}$, we conclude that

$$m_2 p = i^2 + 1 \le \left(\frac{p-1}{2}\right)^2 + 1 < p^2 \tag{30}$$

because $p \ge 5$. Inequality (30) along with the inequality $m_0 \le m_2$ delivers the desired inequality $m_0 < p$, as claimed. □

We recall that $x_0^2 + y_0^2 = m_0 p$; so, next we prove:

Claim 13.3. $\gcd(x_0, m_0) = \gcd(y_0, m_0) = 1$.

Proof of Claim 13.3. We will prove that x_0 and m_0 are coprime; an identical argument (replacing only x_0 with y_0) proves that also y_0 and m_0 are coprime.

So, assume $\gcd(x_0, m_0) > 1$ and thus, let q be a prime dividing both x_0 and m_0. Then $q \mid y_0^2 = m_0p - x_0^2$ and so, $q \mid y_0$. But then $q^2 \mid x_0^2 + y_0^2$ and so, $q^2 \mid m_0p$.

We note that $q < p$ since $m_0 < p$ and $q^2 \mid m_0p$ (which means that $q^2 \le m_0p < p^2$). In particular, $\gcd(q^2, p) = 1$ and because $q^2 \mid m_0p$, then Proposition 2.5 yields that $q^2 \mid m_0$.

So, we let $m_3 := \frac{m_0}{q^2}$; then $m_3 \in \mathbb{N}$. Also, we let $x_1 := \frac{x_0}{q}$ and $y_1 := \frac{y_0}{q}$; then $x_1, y_1 \in \mathbb{Z}$. So, we have

$$x_1^2 + y_1^2 = m_3p,$$

which means that $m_3 \in S$. Because $m_0 = m_3 \cdot q^2$, we get that $m_3 < m_0$, thus contradicting the minimality of m_0; so, indeed, $\gcd(x_0, m_0) = 1$, as desired.

This concludes our proof of Claim 13.3. □

From now on, we assume $m_0 > 1$ and we will derive a contradiction which will therefore prove that m_0 must be equal to 1, i.e., $p = x_0^2 + y_0^2$. Moreover, note that if $p = x_0^2 + y_0^2$, then x_0 and y_0 must be nonzero (because p is not a perfect square); so, letting $a := |x_0|$ and $b = |y_0|$ proves that indeed p is a sum of two perfect squares (of positive integers).

So, we assume now that $m_0 > 1$. Let $x_2, y_2 \in \mathbb{Z}$ satisfying the following two properties:

(i) $x_2 \equiv x_0 \pmod{m_0}$ and $y_2 \equiv y_0 \pmod{m_0}$; and
(ii) $|x_2| \le \frac{m_0}{2}$ and $|y_2| \le \frac{m_0}{2}$.

The existence of x_2 and y_2 satisfying properties (i)-(ii) follows from the fact that for any odd integer $2k + 1$, the set

$$\{-k, k + 1, \cdots, -1, 0, 1, \cdots, k\}$$

represents a complete set of residue classes modulo $2k + 1$, while for an even integer $2k$, the set

$$\{-k, -k + 1, \cdots, -1, 0, 1, \dots, k - 1\}$$

represents a complete set of residue classes modulo $2k$.

Now, for the integers x_2, y_2 satisfying properties (i)-(ii), we observe that

$$x_2 \text{ and } y_2 \text{ are nonzero.} \tag{31}$$

In order to obtain (31), we use the fact proven in claim 13.3 that

$$\gcd(x_0, m_0) = \gcd(y_0, m_0) = 1$$

and also that

$$\gcd(x_2, m_0) = \gcd(y_2, m_0) = 1 \tag{32}$$

because of property (i) above. Furthermore, our assumption that $m_0 > 1$ coupled with (32) yields the desired claim from (31).

Property (i) above along with the fact that $m_0 \mid (x_0^2 + y_0^2)$ yields the existence of some $m_2 \in \mathbb{N}$ such that

$$x_2^2 + y_2^2 = m_0m_2. \tag{33}$$

Property (ii) above yields that

$$m_0m_2 = x_2^2 + y_2^2 \le \frac{m_0^2}{4} + \frac{m_0^2}{4} < m_0^2,$$

which proves that

$$m_2 < m_0. \tag{34}$$

Next we use the identity:

$$(A^2 + B^2)(C^2 + D^2) = (AC + BD)^2 + (AD - BC)^2 \tag{35}$$

and get that

$$(x_0^2 + y_0^2)(x_2^2 + y_2^2) = (x_0x_2 + y_0y_2)^2 + (x_0y_2 - x_2y_0)^2. \tag{36}$$

On one hand, we have (see also (33))

$$(x_0^2 + y_0^2)(x_2^2 + y_2^2) = m_0p \cdot m_0m_2. \tag{37}$$

On the other hand, using that $m_0 \mid x_0^2 + y_0^2$ and also using property (i) above, we get

$$x_0x_2 + y_0y_2 \equiv x_0^2 + y_0^2 \equiv 0 \pmod{m_0}$$

which means that

$$a_0 := \frac{x_0x_2 + y_0y_2}{m_0} \in \mathbb{Z}. \tag{38}$$

Similarly, using property (i) above, we get

$$x_0y_2 - x_2y_0 \equiv x_0y_0 - x_0y_0 \equiv 0 \pmod{m_0},$$

which means that

$$b_0 := \frac{x_0y_2 - x_2y_0}{m_0} \in \mathbb{Z}. \tag{39}$$

Combining (36), (37), (38) and (39), we obtain

$$a_0^2 + b_0^2 = m_2p. \tag{40}$$

So, $m_2 \in S$ (note that $x_2^2 + y_2^2 = m_2p$ and (31) yields that x_2 and y_2 are nonzero, which means that $m_2 \in \mathbb{N}$). But then (34) contradicts the minimality of m_0; so, we got a contradiction, which all started from our assumption that $m_0 > 1$ which allowed us to derive property (31) and eventually get the contradiction from (34) and (40). This concludes our proof of Theorem 13.1. □

Theorem 13.4. *Let n be an integer greater than 1; we write the prime factorization of n as*

$$n = 2^\alpha \cdot \prod_{i=1}^{k} p_i^{\beta_i} \cdot \prod_{j=1}^{\ell} q_j^{\gamma_j}, \tag{41}$$

where α and each β_i and each γ_j are nonnegative integers, while the p_i's are distinct primes of the form $4k+1$ and the q_j's are distinct primes of the form $4k+3$. Then there exist $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = n$ if and only if for each $j = 1, \dots, \ell$, we have that γ_j is even.

Proof. We first prove that whenever n is a sum of two perfect squares, then each γ_j must be even. Indeed, assume $n = a^2 + b^2$ and fix some $q := q_j$ (and also write $\gamma := \gamma_j$); we'll prove that γ must be even.

For any prime p and any nonzero integer m, we denote by $\exp_p(m)$ the exponent of p in m, i.e., writing m as a product of powers of primes, then $\exp_p(m)$ is the exponent in the power of the prime p appearing in the prime factorization of m. If $p \not| m$, then we have $\exp_p(m) = 0$. This

notation for $\exp_p(m)$ will be useful beyond this theorem and will be used throughout the rest of our lectures.

So, with the above notation, we let

$$e := \min\{\exp_q(a), \exp_q(b)\}. \tag{42}$$

Then $q^{2e} \mid a^2+b^2$ and thus $q^{2e} \mid n$, which means that $\gamma \ge 2e$. We let

$$a_1 := \frac{a}{q^e} \text{ and } b_1 := \frac{b}{q^e}$$

and also, $n_1 := \frac{n}{q^{2e}}$; then a_1, b_1, n_1 are integers and we have

$$a_1^2 + b_1^2 = n_1^2.$$

Furthermore, (42) shows that not both a_1 and b_1 are divisible by q. In particular, then corollary 12.2 yields that n_1 cannot be divisible by q (because then that would force that both a_1 and b_1 be divisible by q). So, since $\exp_q(n_1) = 0$, we conclude that $\exp_q(n) = 2e$, i.e., γ is even, as claimed in the conclusion of Theorem 13.4. This proves that if n is a sum of two perfect squares then indeed the exponent of each prime of the form $4k+3$ in the prime power factorization of n must be even.

Next, we assume that each exponent γ_j as in (41) is even and we show that n is indeed a sum of two perfect squares. For this part, we use once again the identity:

$$(A^2+B^2)\cdot(C^2+D^2) = (AC+BD)^2 + (AD-BC)^2, \tag{43}$$

which proves that products of integers which are sums of two perfect squares are once again expressible as sums of two perfect squares. So, for our integer m, we have that

$$2 = 1^2 + 1^2,$$

which combined with (43) proves that 2^α is a sum of perfect squares (note that even if $\alpha = 0$, then still $2^\alpha = 1^2 + 0^2$ is a sum of to perfect squares). Then by Theorem 13.1, we get that each prime p_i is a sum of two perfect squares and then combined with (43), we have that each prime power $p_i^{\beta_i}$ is a sum of two perfect squares. Finally, since each γ_j is even (say, equal to $2e_j$ for some nonnegative integer e_j), then also

$$q_j^{\gamma_j} = \left(q_j^{e_j}\right)^2 + 0^2$$

is a sum of two perfect squares. So, each of 2^α, $p_i^{\beta_i}$ and also $q_j^{\gamma_j}$ is a sum of two perfect squares; then one last application of (43) shows that n is also a sum of two perfect squares, which concludes our proof of Theorem 13.4. □

14. October 24

Theorem 8.2 shows that in order to solve any polynomial congruence equation

$$P(x) \equiv 0 \pmod{m}, \tag{44}$$

where $P \in \mathbb{Z}[x]$, it suffices to split it into finitely many polynomial congruences modulo prime powers; more precisely, letting (for the positive integer m),

$$m := \prod_{i=1}^{r} p_i^{\alpha_i}$$

be its prime powers factorization, then solving (44) is equivalent with solving the system of polynomial congruences modulo prime powers moduli:

$$P(x) \equiv 0 \pmod{p_i^{\alpha_i}} \text{ for } i = 1, \dots, r. \tag{45}$$

So, this shows that we always can reduce to solving a polynomial congruence to the case the moduli m is a prime power p^α. First we will deal with the case of solving polynomial congruences modulo primes (i.e., with the above notation, $\alpha = 1$).

There are two reductions we can always apply when we deal with a polynomial congruence modulo a prime:

$$P(x) \equiv 0 \pmod{p}. \tag{46}$$

Reduction 1. Using Corollary 10.4, we can divide the polynomial $P(x)$ by the polynomial $x^p - x$ and obtain a quotient polynomial $Q \in \mathbb{Z}[x]$ and also a remainder polynomial $R \in \mathbb{Z}[x]$, i.e.,

$$P(x) = (x^p - x) \cdot Q(x) + R(x). \tag{47}$$

Note that the two polynomials Q and R have integer coefficients (and not just rational coefficients which you would generally expect from using the long division of the polynomial $P(x)$ by another polynomial) simply because the polynomial we divide by (i.e., polynomial $x^p - x$) is a *monic* polynomial (i.e., a polynomial whose leading coefficient equals 1). The fact that $Q, R \in \mathbb{Z}[x]$ is an important feature for us; also, important for us is the fact that $\deg(R) < p$ which comes from the long division, which is essentially the Division Algorithm applied inside $\mathbb{Q}[x]$ (which works just as the Division Algorithm we developed for integers, only that the degree of polynomials serves the purpose of ordering the polynomials).

Now, since for any integer a we have that $a^p - a$ is divisible by p (by Corollary 10.4), then (47) shows that if $a \in \mathbb{Z}$ is a solution to congruence equation (46), then we must have that a is a solution to the polynomial congruence equation:

$$R(x) \equiv 0 \pmod{p}. \tag{48}$$

So, solving (46) is the same as solving (48); however, the advantage for us is that the polynomial R has smaller degree than p and therefore, it's likely that solving (48) will be much simpler than solving (46).

Reduction 2. So, we showed in the above reduction, that we may assume that the polynomial $P \in \mathbb{Z}[x]$ from (46) has degree less than p. We write

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0.$$

We claim that we may assume that $P(x)$ is monic, i.e, $a_d = 1$.

Indeed, first of all, we can first assume a_d is not divisible by p since all of the terms in $P(x)$ with coefficients divisible by p may be disregarded since for any $a_j \in \mathbb{Z}$, those terms will always be divisible by p. Now, since we can assume a_d is not divisible by p, then there exists some integer b (not divisible by p) such that

$$a_d \cdot b \equiv 1 \pmod{p},$$

i.e., b is an inverse for a_d modulo p. But then solving (46) is the same as solving the congruence

$$bP(x) \equiv 0 \pmod{p}. \tag{49}$$

Then we can replace each coefficient c of $bP(x)$ with its corresponding representative from the complete set of residue classes $\{0,1,\dots,p-1\}$; in particular, the leading coefficient of $bP(x)$ can be replaced with 1. Hence, we may assume from now on that the leading coefficient of the polynomial in the congruence equation (46) equals 1.

As explained above, we may also assume that each coefficient of the polynomial $P(x)$ from (46) is from the set $\{0,1,\dots,p-1\}$, however in some specific examples, when we work with odd primes p, we may prefer to replace each coefficient of $P(x)$ by the corresponding representative from the complete set of residue classes modulo p: $\{-(p-1)/2,\cdots,-1,0,1,\cdots,(p-1)/2\}$.

So, with the above two reductions, we know that when solving a polynomial congruence equation $P(x)\equiv 0 \pmod{p}$, we may assume $\deg(P)<p$ and that P is monic. However, the next result is true for monic polynomials of arbitrary degree (though it becomes trivial when the degree is at least equal to p).

Theorem 14.1. *Let $P\in\mathbb{Z}[x]$ be a monic polynomial of degree d and let p be a prime number. Then the polynomial congruence equation*

$$P(x)\equiv 0 \pmod{p} \tag{50}$$

has at most d (distinct) solutions.

Proof. We proceed by induction on d. The case when $d=1$ is for monic linear polynomials $P(x):=x+c$ for some $c\in\mathbb{Z}$ and in this case, clearly, the congruence equation (50) has only one solution ($-c$ modulo p).

So, from now on, we assume $d\ge 2$ and furthermore, we assume that Theorem 14.1 holds for all polynomials of degree less than d.

Now, if the congruence equation (50) has no solution, then we're done. So, assume there exists a solution $x_0\in\mathbb{Z}$ of polynomial congruence (50). Then we divide $P(x)$ by $x-x_0$ and obtain quotient $Q(x)$ and remainder $R(x)$, i.e.,

$$P(x)=(x-x_0)\cdot Q(x)+R(x), \tag{51}$$

with $\deg(R)<\deg(x-x_0)=1$, i.e., $R(x):=r\in\mathbb{Z}$ is a constant polynomial (actually, $r=P(x_0)$). However, since $P(x_0)\equiv 0 \pmod{p}$ (according to our assumption), then (51) yields that

$$R(x)\equiv r\equiv 0 \pmod{p}. \tag{52}$$

So, solving (50) reduces (according to (51) and (52)) to the congruence equation

$$(x-x_0)\cdot Q(x)\equiv 0 \pmod{p}. \tag{53}$$

Now, if congruence equation (50) has another solution x_1 which is *different* than x_0 modulo p, i.e.,

$$x_1\not\equiv x_0 \pmod{p}, \tag{54}$$

then (53) (which is equivalent with (50)) yields

$$(x_1-x_0)\cdot Q(x_1)\equiv 0 \pmod{p}. \tag{55}$$

But then (54) and (55) imply that

$$Q(x_1)\equiv 0 \pmod{p}. \tag{56}$$

So, the (distinct modulo p) solutions to congruence equation (50) are x_0 (modulo p) and the solutions to congruence equation (56). However, because of (51), we have that $\deg(Q) = d-1$ and so, the inductive hypothesis tells us that the polynomial congruence equation (56) has at most $d-1$ solutions (modulo p). Therefore, the original congruence equation (50) cannot have more than d distinct solutions modulo p.

This concludes our proof of Theorem 14.1. □

15. October 26

Going from a polynomial congruence equation $P(x) \equiv 0 \pmod{p}$ to another polynomial congruence equation $P(x) \equiv 0 \pmod{p^\alpha}$ (for some integer $\alpha > 1$), we need the following result.

Theorem 15.1. *(Hensel's Lemma) Let p be a prime number, let $f \in \mathbb{Z}[x]$ and let $x_1 \in \mathbb{Z}$ satisfying the following two properties:*

(1) $f(x_1) \equiv 0 \pmod{p}$, *and*
(2) $f'(x_1) \not\equiv 0 \pmod{p}$ *(where $f'(x)$ is the derivative of $f(x)$).*

Then for any $n \in \mathbb{N}$ there exists $x_n \in \mathbb{Z}$ satsfying the following two properties:

(A) $f(x_n) \equiv 0 \pmod{p^n}$, *and*
(B) $x_n \equiv x_1 \pmod{p}$.

Proof. It suffices to argue by induction on n and construct a sequence of integers $\{x_n\}_{n\ge1}$ satisfying the following two properties:

(i) $f(x_n) \equiv 0 \pmod{p^n}$, and
(ii) $x_{n+1} \equiv x_n \pmod{p^n}$

for each $n \ge 1$. Clearly, property (i) is the same as property (A) above, while using repeatedly property (ii), we conclude that property (B) from the conclusion of Theorem 15.1 must hold.

Now, we already know that property (i) holds for $n = 1$ and therefore, all we need to show is that for every $n \ge 1$, if

$$f(x_n) \equiv 0 \pmod{p^n}, \tag{57}$$

then we can choose an integer x_{n+1} satisfying property (ii) for which

$$f(x_{n+1}) \equiv 0 \pmod{p^{n+1}}. \tag{58}$$

So, we let $x_{n+1} = x_n + p^n \cdot \ell$ so that property (ii) would hold; furthermore, since for solving congruence equation (58) all that matters is the residue class of x_{n+1} modulo p^{n+1}, we only need to solve for $\ell \in \{0, \dots, p-1\}$ such that equation (58) holds.

We write

$$f(x) = \sum_{i=0}^{d} c_i x^i,$$

for some integers c_i (and $d \geq 1$). Then

$$\begin{aligned} & f(x_{n+1}) \\ & \qquad = f(x_n + p^n\ell) \\ & \qquad = \sum_{i=0}^{d} c_i \left(x_n + p^n\ell\right)^i \\ & \qquad = \left(\sum_{i=0}^{d} c_i x_n^i\right) + p^n\ell \cdot \sum_{i=1} i c_i x_n^{i-1} + \sum_{i=2}^{d} c_i \sum_{j=2}^{i} x_n^{i-j}\binom{i}{j} \cdot (p^n\ell)^j, \end{aligned}$$

thus proving that

$$f(x_{n+1}) \equiv f(x_n) + p^n\ell \cdot f'(x_n) \pmod{p^{n+1}} \tag{59}$$

since in the last double-sum above each term is divisible by at least p^{2n} (and $2n \geq n+1$). So, in order to achieve (58), we note that (57) yields the existence of an integer $k_n \in \mathbb{Z}$ such that

$$f(x_n) = p^n \cdot k_n. \tag{60}$$

Using (60) in (59), we get that the congruence equation (58) holds if and only if

$$p^{n+1} \mid \left(p^n \cdot k_n + p^n \cdot \ell f'(x_n)\right). \tag{61}$$

However, divisibility (61) is equivalent with the divisibility

$$p \mid k_n + \ell f'(x_n) \text{ i.e.,}$$

$$\ell f'(x_n) \equiv -k_n \pmod{p}. \tag{62}$$

However, our inductive hypothesis tells us that $x_n \equiv x_1 \pmod{p}$ (since condition (ii) above holds for $x_1, \dots, x_n$); so,

$$f'(x_n) \equiv f'(x_1) \pmod{p}, \tag{63}$$

by Proposition 7.1. But then hypothesis (2) shows that $f'(x_n) \not\equiv 0 \pmod{p}$, i.e., $f'(x_n)$ is invertible modulo p. Therefore, the linear congruence equation (62) has a unique solution ℓ modulo p (according to Proposition 7.2). Hence, there exists a unique $\ell \in \{0, \dots, p-1\}$ such that $x_{n+1} = x_n + p^n\ell$ satisfies the congruence equation (58).

This concludes our proof of Theorem 15.1. □

16. October 31

Our focus for most of remaining part of the semester is studying the polynomial congruence equation $x^d \equiv a \pmod{p^\alpha}$ for some given $d \in \mathbb{N}$, $a \in \mathbb{Z}$ not divisible by the prime p, and $\alpha \in \mathbb{N}$.

First we consider the case $\alpha = 1$; after all, using Theorem 15.1, as long as $p \not| d$ (we already assumed $p \not| a$), we can always lift a solution to the congruence equation:

$$x^d \equiv a \pmod{p}$$

to a solution of the congruence equation:

$$x^d \equiv a \pmod{p^\alpha}.$$

Essential for our approach to solving the congruence equation $x^d \equiv a \pmod{p}$ is to know whether there exists some $g \in \mathbb{Z}$ such that the smallest integer e such that $g^e \equiv 1 \pmod{p}$ is $e = p-1$.

Indeed, assuming we can prove that there exists such an integer g, then we obtain that a complete set of nonzero residues modulo p is given by

$$\{1, g, g^2, \cdots, g^{p-2}\}.$$

So, solving the congruence equation

$$x^d \equiv a \pmod{p} \tag{64}$$

reduces to solving a linear congruence equation. Indeed, since $\{1, g, \cdots, g^{p-2}\}$ represents a complete set of nonzero residues modulo p, then there exists some $j \in \{0, 1, \dots, p-2\}$ such that

$$a \equiv g^j \pmod{p}. \tag{65}$$

Also, we're searching for some $x \in \{1, \dots, p-1\}$ solving equation (64); this is the same as searching for some $i \in \{0, 1, \dots, p-2\}$ such that the integer

$$x \equiv g^i \pmod{p} \tag{66}$$

solves the equation (64). So, solving (64) reduces to the congruence equation

$$g^{id} \equiv g^j \pmod{p}. \tag{67}$$

Finally, solving (67) reduces (since $e = p-1$ is the smallest positive integer such that $g^e \equiv 1 \pmod{p}$) to the linear congruence equation

$$di \equiv j \pmod{p-1},$$

which we know precisely how to solve due to Proposition 7.2.

So, our goal for the next several lectures is to prove that for each prime p, there exists an integer g with the property that $e = p-1$ is the smallest positive integer such that $g^e \equiv 1 \pmod{p}$.

Definition 16.1. *Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$ such that $\gcd(a, m) = 1$. We define the order of a modulo m, denoted $\text{ord}_m(a)$ as the smallest positive integer e such that $a^e \equiv 1 \pmod{m}$.*

Note that since $\gcd(a, m) = 1$, Theorem 10.2 yields that $a^{\phi(m)} \equiv 1 \pmod{m}$ and so, we know that the order of a modulo m, as in Definition 16.1 is well-defined; furthermore, $\text{ord}_m(a) \le \phi(m)$.

Proposition 16.2. *Let a and m be nonzero coprime integers. Then for any positive integer e satisfying $a^e \equiv 1 \pmod{m}$, we have that $\text{ord}_m(a) \mid e$.*

Proof. Indeed, we divide the positive integer e (for which $a^e \equiv 1 \pmod{m}$) by $\text{ord}_m(a)$ and obtain quotient q and remainder r, i.e.,

$$e = \text{ord}_m(a) \cdot q + r;$$

we'll prove that r must be 0. Now, we know from Theorem 1.3 that $0 \le r < \text{ord}_m(a)$. On the other hand, we know (since both $a^{\text{ord}_m(a)} \equiv 1 \pmod{m}$ and $a^e \equiv 1 \pmod{m}$) that

$$1 \equiv a^e \equiv \left(a^{\text{ord}_m(a)}\right)^q \cdot a^r \equiv a^r \pmod{m}.$$

So, if $r > 0$, then we get that $a^r \equiv 1 \pmod{m}$ and r is a smaller than $\text{ord}_m(a)$, which is the least positive integer i satisfying $a^i \equiv 1 \pmod{m}$, contradiction. Therefore, we must have $r = 0$, as desired in the conclusion of Proposition 16.2. □

Corollary 16.3. *Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$ be coprime integers. Then $\text{ord}_m(a) \mid \phi(m)$*

Proof. Since $a^{\phi(m)} \equiv 1 \pmod{m}$ (by Theorem 10.2), then Proposition 16.2 delivers the desired conclusion for Corollary 16.3. □

Definition 16.4. *Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$ be coprime integers. We say that a is a primitive root modulo m if $\mathrm{ord}_m(a) = \phi(m)$.*

The immediate goal for us is to prove that for each prime p, there exists some primitive root modulo p. We will even prove that whenever p is an odd prime number and $\alpha \in \mathbb{N}$, there exists a primitive root modulo p^α.

Proposition 16.5. *Let $a \in \mathbb{Z}$ and let $m \in \mathbb{N}$ such that $\gcd(a, m) = 1$. Then for any positive integer n, we have that*

$$\mathrm{ord}_m(a^n) = \frac{\mathrm{ord}_m(a)}{\gcd(n, \mathrm{ord}_m(a))}. \tag{68}$$

Proof. We let $D := \mathrm{ord}_m(a)$ and $d := \gcd(D, n)$. Then both $\frac{D}{d}$ and $\frac{n}{d}$ are positive integers and moreover,

$$(a^n)^{\frac{D}{d}} \equiv \left(a^D\right)^{\frac{n}{d}} \equiv 1^{\frac{n}{d}} \equiv 1 \pmod{m},$$

which proves that the order $D_1 := \mathrm{ord}_m(a^n)$ must satisfy (according to Proposition 16.2 applied to the integer a^n modulo m) the divisibility

$$D_1 \mid \frac{D}{d}. \tag{69}$$

On the other hand, we have

$$a^{D_1 n} \equiv (a^n)^{D_1} \equiv 1 \pmod{m},$$

which proves (once again applying Proposition 16.2, this time applied to the integer a modulo m) the divisibility

$$D \mid D_1 n. \tag{70}$$

Furthermore, since $d = \gcd(D, n)$, we have that the integers $\frac{D}{d}$ and $\frac{n}{d}$ must be coprime. In particular, we get that the divisibility (70) yields

$$\frac{D}{d} \mid \frac{n}{d} \cdot D_1. \tag{71}$$

But using in (71) that $\gcd\left(\frac{D}{d}, \frac{n}{d}\right) = 1$ along with Proposition 2.5, we conclude that

$$\frac{D}{d} \mid D_1. \tag{72}$$

Combining (72) with (69) allows us to conclude that $D_1 = \frac{D}{d}$, as claimed in the conclusion of Proposition 16.5. □

Proposition 16.6. *Let $a_1, a_2 \in \mathbb{Z}$ and $m \in \mathbb{N}$ with the property that*

$$\gcd\left(\mathrm{ord}_m(a_1), \mathrm{ord}_m(a_2)\right) = 1. \tag{73}$$

Then $\mathrm{ord}_m(a_1 a_2) = \mathrm{ord}_m(a_1) \cdot \mathrm{ord}_m(a_2)$.

Proof. We let $d_j := \mathrm{ord}_m(a_j)$ for $j = 1, 2$ and $d := \mathrm{ord}_m(a_1 a_2)$ (note that since a_1 and a_2 are coprime with m, then so is $a_1 \cdot a_2$). We see that

$$(a_1 a_2)^{d_1 d_2} \equiv \left(a_1^{d_1}\right)^{d_2} \cdot \left(a_2^{d_2}\right)^{d_1} \equiv 1^{d_2} \cdot 1^{d_1} \equiv 1 \pmod{m},$$

thus proving (by Proposition 16.2) that

$$d \mid d_1 d_2. \tag{74}$$

Now, on the other hand, since $(a_1 a_2)^d \equiv 1 \pmod{m}$, then we also know that

$$1 \equiv (a_1 a_2)^{dd_1} \equiv \left(a_1^{d_1}\right)^d \cdot a_2^{dd_1} \equiv 1 \cdot a_2^{dd_1} \equiv a_2^{dd_1} \pmod{m}.$$

So, then using Proposition 16.2 to a_2 for which we know that $a_2^{dd_1} \equiv 1 \pmod{m}$, we conclude that

$$d_2 \mid dd_1. \tag{75}$$

But then using Proposition 2.5 (note that d_1 and d_2 are coprime) to divisibility (75), we conclude that

$$d_2 \mid d. \tag{76}$$

Running the exact same argument but applied to a_2 instead of a_1, we derive that $d_1 \mid d$. Indeed,

$$1 \equiv (a_1 a_2)^{dd_2} \equiv (a_1)^{dd_2} \cdot \left(a_2^{d_2}\right)^d \equiv a_1^{dd_2} \cdot 1 \equiv a_1^{dd_2} \pmod{m}$$

and so, $d_1 \mid dd_2$ and because $\gcd(d_1, d_2) = 1$, we conclude that

$$d_1 \mid d. \tag{77}$$

Equations (76) and (77) coupled with the fact that d_1 and d_2 are coprime yields that

$$d_1 d_2 \mid d. \tag{78}$$

Equations (74) and (78) show that indeed, $d = d_1 d_2$, as desired in the conclusion of Proposition 16.6. □

17. November 2

Proposition 17.1. *Let p be a prime and $d \in \mathbb{N}$ a divisor of $p-1$. Then the polynmial congruence equation*

$$x^d \equiv 1 \pmod{p} \tag{79}$$

has precisely d solutions.

Proof. First of all, Theorem 14.1 yields that congruence equation (79) doesn't have more than d solutions. On the other hand, we know that the congruence equation

$$x^{p-1} \equiv 1 \pmod{p}$$

has precisely $p-1$ solutions $\{1, \ldots, p-1\}$ modulo p. We see that

$$x^{p-1} - 1 = (x^d - 1) \cdot \left(x^{p-1-d} + x^{p-1-2d} + \cdots + x^d + 1\right)$$

and so, for each integer $i \in \{1, \ldots, p-1\}$ satisfying $i^{p-1} \equiv 1 \pmod{p}$, it means that

$$\text{either } p \mid i^d - 1 \tag{80}$$

$$\text{or } p \mid \left(i^{p-1-d} + i^{p-1-2d} + \cdots + i^d + 1\right). \tag{81}$$

However, another application of Theorem 14.1 applied to (81) yields that there cannot be more than $p-1-d$ integers $i \in \{1, \ldots, p-1\}$ satisfying divisibility (81). In conclusion, there must be d integers $i \in \{1, \ldots, p-1\}$ satisfying divisibility (80).

So, indeed, as claimed in Proposition 17.1, there are precisely d solutions to the congruence equation (79). □

Proposition 17.2. *Let p and q be primes and α be a positive integer such that $q^\alpha \mid p-1$. Then there exists $a \in \mathbb{Z}$ such that $\operatorname{ord}_p(a) = q^\alpha$.*

Proof. By Proposition 17.1, we know that there exist q^α solutions to the congruence equation

$$x^{q^\alpha} \equiv 1 \pmod{p}. \tag{82}$$

Now, for any of these q^α solutions x_1 to congruence equation (82), if $\operatorname{ord}_p(x_1) \neq q^\alpha$, then we still have (according to Proposition 16.2) that $\operatorname{ord}_p(x_1)$ is a power of q; so, if $\operatorname{ord}_p(x_1) \neq q^\alpha$, then we must have that $\operatorname{ord}_p(x_1) = q^\beta$ for some $\beta \le \alpha - 1$. Thus

$$x_1^{q^{\alpha-1}} \equiv 1 \pmod{p}, \tag{83}$$

because $\operatorname{ord}_p(x) \mid q^{\alpha-1}$ in this case. However, according to Proposition 17.1, there are precisely $q^{\alpha-1}$ solutions to the congruence equation (83). In conclusion, all solutions to congruence equation (82), which are **not** also solutions to congruence equation (83) must be an integer of order precisely q^α modulo p; as shown by Proposition 17.1 applied to the two congruence equations (82) and (83), there are $q^\alpha - q^{\alpha-1}$ such integers modulo p of order q^α.

This concludes our proof of Proposition 17.2. □

Theorem 17.3. *Let p be a prime number. Then there exist precisely $\phi(p-1)$ distinct residue classes modulo p containing integers a with the property that $\operatorname{ord}_a(p) = p-1$.*

Proof. We write $\phi(p-1) = \prod_{j=1}^{\ell} q_j^{\beta_j}$ (its prime power factorization). Then by Proposition 17.2 yields that for each $j = 1, \dots, \ell$, there exists some integer a_j with $\operatorname{ord}_p(a_j) = q_j^{\beta_j}$. But then (since the primes q_j are distinct), Proposition 16.6 (applied repeatedly) yields that

$$\operatorname{ord}_p\left(\prod_{j=1}^{\ell} a_j\right) = \prod_{j=1}^{\ell} q_j^{\beta_j} = p-1.$$

So, there exist primitive elements modulo p; next we prove that there exist $\phi(p-1)$ such primitive elements modulo p.

Now, the fact that we have an integer g of order $p-1$ modulo p means that the nonzero residue classes modulo p may also be represented by the integers:

$$\{1, g, g^2, \cdots, g^{p-2}\}.$$

So, for an integer in the residue class of g^i (for $i \in \{0, \dots, p-2\}$), we have that its order modulo p is $p-1$ if

$$\operatorname{ord}_p(g^i) = p-1. \tag{84}$$

However, Proposition 16.5 yields that

$$\operatorname{ord}_p(g^i) = \frac{\operatorname{ord}_p(g)}{\gcd(i, \operatorname{ord}_p(g))} = \frac{p-1}{\gcd(i, p-1)}.$$

Coupling this last formula with (84), we obtain that g^i is also a primitive element modulo p if and only if $\gcd(i, p-1) = 1$; therefore, there exist precisely $\phi(p-1)$ integers i from $\{0, 1, \dots, p-2\}$ such that g^i has order $p-1$ modulo p.

This concludes our proof of Theorem 17.3. □

18. November 7

Theorem 18.1. *Let p be an odd prime number and let $\alpha \in \mathbb{N}$. Then there exists an integer a with $\operatorname{ord}_{p^\alpha}(a) = \phi(p^\alpha)$.*

Proof. We already established in Theorem 17.3 that there exists $g_1 \in \mathbb{Z}$ whose order modulo p is indeed $p-1$. Next we show that there exists an integer g_2 of order $\phi(p^2)$ modulo p^2, where $g_2 = g_1 + p\ell$ for a suitable $\ell \in \{0, \dots, p-1\}$.

First of all, letting $d_2 = \operatorname{ord}_{p^2}(g_2)$, we see that $g_2^{d_2} \equiv 1 \pmod{p^2}$ and so, $g_2^{d_2} \equiv 1 \pmod{p}$. Because $g_2 \equiv g_1 \pmod{p}$, we also have

$$g_1^{d_2} \equiv 1 \pmod{p}. \tag{85}$$

Using (85) coupled with Proposition 16.2 (and the fact that $\operatorname{ord}_p(g_1) = p-1$), we get that

$$p-1 \mid d_2. \tag{86}$$

The using (86), in order to prove that $d_2 = \phi(p^2) = p(p-1)$, all we need to show is that $d_2 \neq p-1$; in other words, we need to find some $\ell \in \{0, \dots, p-1\}$ such that

$$g_2^{p-1} \not\equiv 1 \pmod{p^2}. \tag{87}$$

Now, g_2 is coprime with p; so, we see that (87) holds if and only if

$$g_2^p \not\equiv g_2 \pmod{p^2}. \tag{88}$$

(All we're using is that $p^2 \not| (g_2^{p-1} - 1)$ if and only if $p^2 \not| g_2 \cdot (g_2^{p-1} - 1)$ because $\gcd(p, g_2) = 1$.)

Now, we compute

$$\begin{aligned} g_2^p & \\ &= (g_1 + p\ell)^p \\ &= g_1^p + \binom{p}{1} \cdot p\ell g_1^{p-1} + \sum_{i=2}^{p} g_i^{p-i} \binom{p}{i} \cdot (p\ell)^i, \end{aligned}$$

which proves (since $\binom{p}{1} = p$) that

$$g_2^p \equiv g_1^p \pmod{p^2}. \tag{89}$$

Since our goal is to find some $\ell \in \{0, \dots, p-1\}$ such that (88) holds, then we need the following:

$$g_1^p \not\equiv g_1 + p\ell \pmod{p^2}. \tag{90}$$

Now, we know (see Corollary 10.4) that $g_1^p \equiv g_1 \pmod{p}$, i.e, there exists some $k_1 \in \mathbb{Z}$ such that $g_1^p - g_1 = pk_1$. Thus, we achieve (90) if

$$pk_1 \not\equiv p\ell \pmod{p^2}, \text{ i.e.,}$$

$$k_1 \not\equiv \ell \pmod{p}. \tag{91}$$

There are $p-1$ possible values for $\ell \in \{0, \dots, p-1\}$ satisfying (91) and thus, there exists $g_2 \in \mathbb{Z}$ satisfying (87); so, we proved the existence of an integer g_2, which is a primitive root modulo p^2.

We will prove that g_2 (constructed above) is also primitive modulo p^α for any $\alpha \ge 2$. We argue by induction on α; the case $\alpha = 2$ being just established. So, we assume that we proved (for some $\alpha \ge 2$) that

$$\mathrm{ord}_{p^\alpha}(g_2) = \phi(p^\alpha) = p^{\alpha-1}(p-1) \tag{92}$$

and we prove next that

$$\mathrm{ord}_{p^{\alpha+1}}(g_2) = \phi\left(p^{\alpha+1}\right) = p^\alpha(p-1). \tag{93}$$

We let $d_{\alpha+1} := \mathrm{ord}_{p^{\alpha+1}}(g_2)$; so, $g_2^{d_{\alpha+1}} \equiv 1 \pmod{p^{\alpha+1}}$ and in partcular,

$$g_2^{d_{\alpha+1}} \equiv 1 \pmod{p^\alpha},$$

which combined with Proposition 16.2 yields

$$\mathrm{ord}_{p^\alpha}(g_2) \mid d_{\alpha+1}. \tag{94}$$

Combining (92) with (94), we obtain

$$p^{\alpha-1}(p-1) \mid d_{\alpha+1}. \tag{95}$$

On the other hand, clearly by Corollary 16.3, we have that

$$d_{\alpha+1} \mid \phi(p^{\alpha+1}) = p^\alpha(p-1). \tag{96}$$

So, combining (95) with (96), in order to achieve that $d_{\alpha+1} = \phi(p^{\alpha+1})$, all we need to prove is that $d_{\alpha+1} \ne p^{\alpha-1}(p-1)$, i.e.,

$$g_2^{p^{\alpha-1}(p-1)} \not\equiv 1 \pmod{p^{\alpha+1}}. \tag{97}$$

On the other hand, we know that $\mathrm{ord}_{p^\alpha}(g_2) = \phi(p^\alpha) = p^{\alpha-1}(p-1)$, i.e.,

$$g_2^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}. \tag{98}$$

However, we do know that (since $\alpha \ge 2$ and so, $\phi(p^{\alpha-1}) = p^{\alpha-2}(p-1)$)

$$g_2^{p^{\alpha-2}(p-1)} \equiv 1 \pmod{p^{\alpha-1}}. \tag{99}$$

Combining (98) with (99), we get the existence of some integer r **not divisible** by p such that

$$g_2^{p^{\alpha-2}(p-1)} = 1 + rp^{\alpha-1}.$$

Thus

$$\begin{aligned} & g_2^{p^{\alpha-1}(p-1)} \\ & \qquad = \left(1 + rp^{\alpha-1}\right)^p \\ & \qquad = 1 + p \cdot rp^{\alpha-1} + \left(\sum_{i=2}^{p-1} \binom{p}{i} \cdot \left(rp^{\alpha-1}\right)^i\right) + \left(rp^{\alpha-1}\right)^p. \end{aligned}$$

Now, for each $i = 2, \dots, p-1$, we have that $p \mid \binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1\cdot 2\cdots i}$ and therefore, the exponent of p in each term of the above parenthesis (for $i = 2, \dots, p-1$) is at least

$$1 + 2(\alpha - 1) = (\alpha + 1) + (\alpha - 2) \ge \alpha + 1,$$

because $\alpha \ge 2$. Also, the exponent of the prime p in the last term of the above sum is

$$p(\alpha - 1) \ge 3(\alpha - 1) = \alpha + 1 + 2(\alpha - 2) \ge \alpha + 1,$$

because not only $\alpha \geq 2$ but also $p \geq 3$ (since p is an odd prime number). In conclusion, we obtain that

$$g_2^{p^{\alpha-1}(p-1)} - 1 \equiv rp^{\alpha} \not\equiv 0 \pmod{p^{\alpha+1}} \tag{100}$$

because $p \not| r$. So, (100) delivers the desired information about $d_{\alpha+1}$ that it cannot be $p^{\alpha-1}(p-1)$; hence, (95) yields that

$$\mathrm{ord}_{p^{\alpha+1}}(g_2) = p^{\alpha}(p-1) = \phi\left(p^{\alpha+1}\right),$$

as claimed in the conclusion of Theorem 18.1. □

Proposition 18.2. *Let p be an odd prime number, let a be an integer not divisible by p, and let n and α be positive integers; we let $d = \gcd(n, \phi(p^{\alpha}))$. Then the number of solutions to the congruence equation*

$$x^n \equiv a \pmod{p^{\alpha}} \tag{101}$$

is

$$\begin{cases} 0 & \text{if} \quad a^{\frac{\phi(p^{\alpha})}{d}} \not\equiv 1 \pmod{p^{\alpha}} \\ d & \text{if} \quad a^{\frac{\phi(p^{\alpha})}{d}} \equiv 1 \pmod{p^{\alpha}} \end{cases}$$

Proof. Since p is an odd prime, then there exists a primitive root g modulo p^{α} (according to Theorem 18.1). So, all the residue classes modulo p^{α} containing integers coprime with p are represented by the integers from the set

$$\left\{g^i \colon 0 \leq i \leq \phi\left(p^{\alpha}\right) - 1\right\}.$$

So, since $p \not| a$, there exists $j \in \{0, \dots, p^{\alpha-1}(p-1)-1\}$ such that $a \equiv g^j \pmod{p^{\alpha}}$. Similarly, in order to solve congruence equation (101), it suffices to find some $i \in \{0, \dots, p^{\alpha-1}(p-1)-1\}$ such that for $x \equiv g^i \pmod{p^{\alpha}}$, we would have

$$x^n \equiv a \pmod{p^{\alpha}}, \text{ i.e.,}$$

$$g^{ni} \equiv g^j \pmod{p^{\alpha}}. \tag{102}$$

Claim 18.3. *With the above notation for p, α and g, given nonnegative integers a and b, we have that $g^a \equiv g^b \pmod{p^{\alpha}}$ if and only if $a \equiv b \pmod{\phi(p^{\alpha})}$.*

Proof of Claim 18.3. Without loss of generality, we may assume $b \geq a$ (otherwise we swap a and b). So, the congruence $g^a \equiv g^b \pmod{p^{\alpha}}$ is equivalent with

$$p^{\alpha} \mid g^b - g^a, \text{ i.e.,}$$

$$p^{\alpha} \mid g^a(g^{b-a} - 1). \tag{103}$$

Using (103) along with Proposition 2.5 (note that $\gcd(p^{\alpha}, g) = 1$), we conclude that

$$p^{\alpha} \mid g^{b-a} - 1. \tag{104}$$

Since $\mathrm{ord}_{p^{\alpha}}(g) = \phi(p^{\alpha})$, then divisibility (104) along with Proposition 16.2 yields the desired conclusion for Claim 18.3.

Finally, if $b - a$ is a multiple of $\phi(p^{\alpha})$, then clearly divisibility (103) holds and therefore, $g^a \equiv g^b \pmod{p^{\alpha}}$. This concludes our proof for Claim 18.3. □

Now, Claim 18.3 shows that congruence equation (102) is equivalent with

$$ni \equiv j \pmod{\phi(p^\alpha)}. \tag{105}$$

Then the conclusion of Proposition 18.2 follows immediately from Proposition 7.2. Indeed, we get that (105) is solvable precisely when $d = \gcd(n, \phi(p^\alpha))$ divides j (and when it is solvable, there are d solutions to the linear congruence equation (105)). On the other hand, Proposition 16.5 (along with the fact that $\mathrm{ord}_{p^\alpha}(g) = \phi(p^\alpha)$) shows that

$$\mathrm{ord}_{p^\alpha}(g^j) = \frac{\phi(p^\alpha)}{\gcd(\phi(p^\alpha), j)} \tag{106}$$

and so, $d \mid j$ if and only if the integer $\frac{\phi(p^\alpha)}{\gcd(\phi(p^\alpha),j)}$ divides the integer $\frac{\phi(p^\alpha)}{d}$ (note that $d \mid \phi(p^\alpha)$) if and only if (using also Proposition 16.2)

$$(g^j)^{\frac{\phi(p^\alpha)}{d}} \equiv 1 \pmod{p^\alpha}.$$

This concludes our proof of Proposition 18.2. □

The following results are immediate consequences of Proposition 18.2.

Corollary 18.4. *Let p be an odd prime number, let a be an integer not divisible by p, and let n be a positive integers; we let $d = \gcd(n, p-1)$. Then the number of solutions to the congruence equation*

$$x^n \equiv a \pmod p$$

is

$$\begin{cases} 0 & \textit{if} \quad a^{\frac{p-1}{d}} \not\equiv 1 \pmod p \\ d & \textit{if} \quad a^{\frac{p-1}{d}} \equiv 1 \pmod p \end{cases}$$

Corollary 18.5. *Let p be an odd prime and let $a \in \mathbb{Z}$ not divisible by p. Then the number of solutions to the congruence equation*

$$x^2 \equiv a \pmod p$$

is

$$\begin{cases} 0 & \textit{if} \quad a^{\frac{p-1}{2}} \not\equiv 1 \pmod p \\ 2 & \textit{if} \quad a^{\frac{p-1}{2}} \equiv 1 \pmod p \end{cases}$$

19. November 14

From now on, unless otherwise noted, the prime p is always assumed to be odd.

Definition 19.1. *Let p be an odd prime and let $a \in \mathbb{Z}$. We define the Legendre symbol $\left(\frac{a}{p}\right)$ as follows*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \textit{if} \quad p \mid a \\ 1 & \textit{if} \quad p \not| a \textit{ and the congruence equation } x^2 \equiv a \pmod p \textit{ is solvable} \\ -1 & \textit{if} \quad \textit{the congruence equation } x^2 \equiv a \pmod p \textit{ is not solvable} \end{cases}$$

If $\left(\frac{a}{p}\right) \in \{0,1\}$, we say that a is a quadratic residue modulo p, while if $\left(\frac{a}{p}\right) = -1$, we say that a is not a quadratic residue (or a non-quadratic residue) modulo p.

For example, $\left(\frac{14}{7}\right) = 0$ (since $7 \mid 14$), $\left(\frac{4}{7}\right) = 1$ (because 4 is already a perfect square), $\left(\frac{2}{7}\right) = 1$ (because the congruence equation $x^2 \equiv 2 \pmod 7$ is solved by $x \equiv \pm 3 \pmod 7$), while $\left(\frac{3}{7}\right) = -1$ (because the congruence equation $x^2 \equiv 3 \pmod 7$ is unsolvable).

Proposition 19.2. *For any odd prime p and any integer a, we have that*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p. \tag{107}$$

Proof. If $p \mid a$ then (107) holds immediately since both sides are congruent with 0 modulo p. So, from now on, we assume $p \not| a$.

Now, the congruence equation $x^2 \equiv a \pmod p$ is solvable if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ (according to Corollary 18.5). In particular, whenever $x^2 \equiv a \pmod p$ is unsolvable, we have $a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$. However, since Theorem 10.3 yields

$$a^{p-1} \equiv 1 \pmod p,$$

then $p \mid \left(a^{\frac{p-1}{2}} - 1\right) \cdot \left(a^{\frac{p-1}{2}} + 1\right)$. So, since in this case we have $p \not| a^{\frac{p-1}{2}} - 1$, then we must have

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p,$$

as claimed in the conclusion of Proposition 19.2. □

The following properties of the Legendre symbol are easy consequences of its definition and of Proposition 19.2; however, they are very often used in applications.

Proposition 19.3. *Given an odd prime number p, the following properties hold:*

(i) *for any integer a not divisible by p, we have $\left(\frac{a^2}{p}\right) = 1$; in particular, $\left(\frac{1}{p}\right) = 1$.*

(ii) *$\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1 \pmod 4$ and $\left(\frac{-1}{p}\right) = -1$ if $p \equiv -1 \pmod 4$.*

(iii) *$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ for any integers a and b.*

(iv) *if $p \not| a$, then $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.*

Proof. Property (i) is clear from Definition 19.1. Property (ii) follows from Properties 11.3 and 12.1. Also, property (iv) is an immediate consequence of property (iii) coupled with property (i). So, we're left now to proving property (iii).

Now, by Proposition 19.2, we have that

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \pmod p. \tag{108}$$

But since the Legendre symbol for any integer modulo p is a number in the set $\{-1, 0, 1\}$, we have that

$$\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \in \{-2, -1, 0, 1, 2\}. \tag{109}$$

However, since $p \geq 3$, congruence equation (108) coupled with equation (109) yields that

$$\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = 0, \tag{110}$$

as desired in the conclusion of Proposition 19.3. □

All the nonzero quadratic residues modulo p are in the set of residues modulo p given by

$$\left\{1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2\right\}. \tag{111}$$

Indeed, since a complete set of nonzero residues modulo p is given by the set of all integers $\pm i$ for $1 \le i \le \frac{p-1}{2}$, we see that the only possible nonzero quadratic residues modulo p are the ones given by the set (111). Furthermore, we claim that for any

$$1 \le i < j \le \frac{p-1}{2}, \tag{112}$$

we have that $i^2 \not\equiv j^2 \pmod{p}$. Indeed,

$$j^2 - i^2 = (j-i)(j+i)$$

and both $j-i$ and $j+i$ are contained in the set $\{1, 2, \dots, p-1\}$ due to inequalities (112). So, p cannot divide $j^2 - i^2 = (j-1)(j+i)$, thus proving that all the numbers i^2 (for $i = 1, \dots, \frac{p-1}{2}$) are distinct modulo p. Therefore, there exist precisely $\frac{p-1}{2}$ nonzero quadratic residues and precisely $\frac{p-1}{2}$ non-quadratic residues modulo p. This allows us easily to conclude the following:

Proposition 19.4. *Let p be an odd prime number. Then*

$$\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0. \tag{113}$$

Proposition 19.5. *Let p be an odd prime number. Then $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, i.e.,*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if} \quad p \equiv \pm 1 \pmod{8} \\ -1 & \text{if} \quad p \equiv \pm 3 \pmod{8} \end{cases}$$

Proof. We know that a complete set of representatives for the nonzero residue classes modulo p is

$$\left\{-\frac{p-1}{2}, -\frac{p-3}{2}, \cdots, -1, 0, 1, \cdots, \frac{p-3}{2}, \frac{p-1}{2}\right\}.$$

So, for each $i \in \{1, \dots, \frac{p-1}{2}\}$, there exists a unique $\epsilon(i) \in \{0, 1\}$ and a unique $f(i) \in \{1, \dots, \frac{p-1}{2}\}$ such that

$$2i \equiv (-1)^{\epsilon(i)} \cdot f(i) \pmod{p}. \tag{114}$$

Claim 19.6. *The function $f : \{1, \dots, \frac{p-1}{2}\} \longrightarrow \{1, \dots, \frac{p-1}{2}\}$ is bijective.*

Proof of Claim 19.6. **Since f is a function from a finite set into itself, in order to prove that it's bijective, it suffices to prove that f is injective.**

So, assume $f(i) = f(j)$ for some $i, j \in \{1, \dots, \frac{p-1}{2}\}$. There are then two possibilities:

Case 1. $\epsilon(i) = \epsilon(j)$.

In this case, since also $f(i) = f(j)$, then (114) yields that

$$2i \equiv 2j \pmod{p}. \tag{115}$$

Because p is odd and thus, 2 is invertible modulo p and thus Corollary 6.4 yields that $i \equiv j \pmod{p}$. Since $i, j \in \{1, \dots, \frac{p-1}{2}\}$, then we must have $i = j$, as claimed.

Case 2. $\epsilon(i) \neq \epsilon(j)$.

Then $(-1)^{\epsilon(i)} = -(-1)^{\epsilon(j)}$ and since $f(i) = f(j)$, then (114) yields that

$$2i \equiv -2j \pmod{p}. \tag{116}$$

Since $\gcd(2,p) = 1$, (116) yields that $p \mid i+j$. However, $i,j \in \{1,\dots,\frac{p-1}{2}\}$, contradiction.

Hence, we must have that $f(i) = f(j)$ if and only if $i = j$, i.e., f is injective and therefore bijective, which concludes our proof of Claim 19.6. □

Claim 19.6 shows that letting s be the number of all $i \in \{1,\dots,\frac{p-1}{2}\}$ for which $\epsilon(i) = 1$, then we must have that

(117)

$$2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv \prod_{i=1}^{\frac{p-1}{2}} (2i) \equiv \prod_{i=1}^{\frac{p-1}{2}} \Big((-1)^{\epsilon(i)} \cdot f(i)\Big) \equiv (-1)^s \cdot \prod_{i=1}^{\frac{p-1}{2}} i \equiv (-1)^s \cdot \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Using the fact that $\left(\frac{p-1}{2}\right)!$ is invertible modulo p (and Corollary 6.4) in congruence equation (117) allows us to conclude that

$$2^{\frac{p-1}{2}} \equiv (-1)^s \pmod{p}. \tag{118}$$

Using (118) and Proposition 19.2, then all we need to prove is that

$$(-1)^s = \begin{cases} 1 & \text{if} \quad p \equiv \pm 1 \pmod{8} \\ -1 & \text{if} \quad p \equiv \pm 3 \pmod{8} \end{cases}$$

We also know that

$$s = \#\left\{1 \leq i \leq \frac{p-1}{2} : 2i > \frac{p-1}{2}\right\}$$

since $\epsilon(i) = 1$ precisely when $2i > \frac{p-1}{2}$ (otherwise, simply $\epsilon(i) = 0$ and $f(i) = 2i$). In order to prove the above formula for $(-1)^s$, we'll split our analysis into two cases depending on p being of the form $4k+1$ or $4k+3$.

Case 1. $p = 4k+1$ for some $k \in \mathbb{N}$.

In this case, we have

$$s = \#\{1 \leq i \leq 2k \colon 2i > 2k\} = \#\{k+1,\dots,2k\} = k.$$

So, $(-1)^s = 1$ precisely when k is even, i.e., when $p \equiv 1 \pmod{8}$ and $(-1)^s = -1$ precisely when k is odd, i.e., when $p \equiv 5 \pmod{8}$.

Case 2. $p = 4k+3$ for some nonzero integer k.

In this case, we have

$$s = \#\{1 \leq i \leq 2k+1 \colon 2i > 2k+1\} = \#\{k+1,\dots,2k+1\} = k+1.$$

So, $(-1)^s = 1$ precisely when k is odd, i.e., when $p \equiv 7 \pmod{8}$ and $(-1)^s = -1$ precisely when k is even, i.e., when $p \equiv 3 \pmod{8}$.

This concludes our proof of Proposition 19.5. □

Theorem 19.7. *(Gauss Quadratic Reciprocity Law) Let $p \neq q$ be odd prime numbers. Then*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}. \tag{119}$$

Equation (119) is equivalent with asking that

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}} \tag{120}$$

or alternatively, writing that

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{if} \qquad\qquad p \equiv q \equiv -1 \pmod 4 \\ \left(\frac{q}{p}\right) & \text{if} \quad \text{either } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \end{cases}$$

We will spend the next several lectures proving Theorem 19.7.

20. November 16

Proposition 20.1. *Let p be an arbitrary prime number and let $f, g \in \mathbb{Z}[x]$ with the property that each coefficient in the polynomial $h(x) := f(x) \cdot g(x)$ is divisible by p. Then prove that either each coefficient of $f(x)$ is divisible by p, or each coefficient of $g(x)$ is divisible by p.*

Proof. We write $f(x) := \sum_{i=0}^{m} a_i x^i$ and $g(x) := \sum_{j=0}^{n} b_j x^j$ for coefficients $a_i, b_j \in \mathbb{Z}$. We argue by contradiction and therefore, assume there exists $k \in \{0, \dots, m\}$ and $\ell \in \{0, \dots, n\}$ such that

$$p \not| a_k \text{ and also } p \not| b_\ell. \tag{121}$$

Furthermore, we may assume k is the largest index (in the range $\{0, \dots, m\}$) and also ℓ is the largest index (in the range $\{0, \dots, n\}$) satisfying (121). So, in particular, we have

$$p \mid a_i \text{ for } i > k \text{ and } p \mid b_j \text{ for } j > \ell. \tag{122}$$

But then computing the coefficient $c_{k+\ell}$ in $f(x) \cdot g(x)$ for the term involving $x^{k+\ell}$, we obtain

$$c_{k+\ell} = \sum_{\substack{i+j=k+\ell \\ 0 \le i \le m \\ 0 \le j \le n}} a_i b_j = a_k b_\ell + \sum_{\substack{i+j=k+\ell \\ 0 \le i \le m \\ 0 \le j \le n \\ i>m \text{ or } j>n}} a_i b_j. \tag{123}$$

Using (121) and (122) in (123) allow us to conclude that $p \not| c_{k+\ell}$, contradiction. Therefore, indeed, either all coefficients of $f(x)$ or all coefficients of $g(x)$ must be divisible by p. □

Theorem 20.2. *(Gauss's lemma) Let $f(x) \in \mathbb{Z}[x]$. Then there exist $g, h \in \mathbb{Z}[x]$ satisfying the two properties:*

(a) *$f(x) = g(x) \cdot h(x)$, and*
(b) *$\deg(g) < \deg(f)$ and $\deg(h) < \deg(f)$*

if and only if there exist $G, H \in \mathbb{Q}[x]$ satisfying the two properties:

(A) *$f(x) = G(x) \cdot H(x)$, and*
(B) *$\deg(G) < \deg(f)$ and $\deg(H) < \deg(f)$.*

Essentially, Theorem 20.2 says that a polynomial with integer coefficients is *irreducible* (i.e., it cannot be written as a product of two polynomials of smaller degree) in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$. Therefore, from now on, for a polynomial $f(x)$ with integer coefficients, when we say that f is irreducible, we do not need to specify whether

this means irreducible in $\mathbb{Z}[x]$ or in $\mathbb{Q}[x]$, since both notions coincide for us.

Very important: we do not consider the polynomial $2x^2+6$ be reducible in $\mathbb{Z}[x]$ because we can write it as $2\cdot(x^2+3)$; instead the polynomial $2x^2+6$ will be - for us - irreducible both in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$ because it cannot be written as a product of two polynomials of *smaller* degree, either in $\mathbb{Z}[x]$ or in $\mathbb{Q}[x]$.

Proof of Theorem 20.2. Clearly, if conditions (a) and (b) are met, then also conditions (A) and (B) are met. So, all we have to prove is that if there exist polynomials $G, H \in \mathbb{Q}[x]$ satisfying conditions (A) and (B), then we can also find polynomials $g, h \in \mathbb{Z}[x]$ satisfying conditions (a) and (b).

Claim 20.3. *Let $F \in \mathbb{Q}[x]$. Then there exist coprime integers D_F and N_F along with some polynomial $\tilde{F} \in \mathbb{Z}[x]$ such that*

- *$F(x) = \frac{N_F}{D_F} \cdot \tilde{F}(x)$, and*
- *the greatest common divisor of all coefficients of $\tilde{F}(x)$ equals 1.*

Proof of Claim 20.3. First, we can write $F(x)$ as $\frac{F_1(x)}{D_1}$, where $D_1 \in \mathbb{N}$ and $F_1 \in \mathbb{Z}[x]$ (simply by clearing the denominators of the coefficients of $F(x)$). Then we let N_1 be the greatest common divisor of all coefficients of $F_1(x)$; so,

$$\tilde{F}(x) := \frac{F_1(x)}{N_1} \in \mathbb{Z}[x].$$

Furthermore, the greatest common divisor of all the coefficients of $\tilde{F}(x)$ must be equal to 1. Finally, we write the rational number $\frac{N_1}{D_1}$ in lowest terms as $\frac{N_F}{D_F}$ (for some coprime integers N_F and D_F) and therefore obtain the desired conclusion in Claim 20.3. □

Using Claim 20.3 for the polynomials G and H, we obtain the polynomials $\tilde{G}(x)$ and $H\tilde{(}x)$ with integer coefficients (whose greatest common divisors for their coefficients equal 1, both for $\tilde{G}(x)$ and for $\tilde{H}(x)$), along with integers N_G, N_H, D_G, D_H such that

$$G(x) = \frac{N_G}{D_G} \cdot \tilde{G}(x) \text{ and } H(x) = \frac{N_H}{D_H} \cdot \tilde{H}(x). \tag{124}$$

Then we find coprime integers a and b (with b positive, while a can be either positive or negative) such that

$$\frac{a}{b} := \frac{N_G \cdot N_H}{D_G \cdot D_H}. \tag{125}$$

Using (124) and (125) in condition (A), yields that

$$f(x) = \frac{a}{b} \cdot \tilde{G}(x) \cdot \tilde{H}(x). \tag{126}$$

Therefore, all coefficients in $bf(x) = a\tilde{G}(x)\tilde{H}(x)$ are divisible by b.

If $b = 1$, then we are done; we could simply choose $g(x) := a\tilde{G}(x) \in \mathbb{Z}[x]$ and $h(x) := \tilde{H}(x) \in \mathbb{Z}[x]$ and get that f and g satisfy conditions (a)-(b) above (note that $\deg(g) = \deg(\tilde{G}) = \deg(G) < \deg(f)$ and also $\deg(h) = \deg(\tilde{H}) = \deg(H) < \deg(f)$ according to condition (B) for G and H).

Now, assume $b > 1$; then there exists a prime p dividing b. But then p divides each coefficient of $bf(x) = \left(a\tilde{G}(x)\right) \cdot \tilde{H}(x)$; so, by Proposition 20.1, p must divide either each coefficient in $a\tilde{G}(x)$ or each coefficient in $\tilde{H}(x)$. However, we already know that the greatest common divisor of all coefficients in $\tilde{H}(x)$ equals 1; so, it means that p divides each coefficient of $a\tilde{G}(x)$. But $p \mid b$ and $\gcd(a, b) = 1$ (by our choice of a and b); thus $p \nmid a$, which means that p must divide each coefficient in $\tilde{G}(x)$. However, this is again impossible due to the fact that the greatest common divisor for all coefficients in $\tilde{G}(x)$ equals 1.

In conclusion, $b = 1$ and thus, $f(x)$ is also reducible in $\mathbb{Z}[x]$, as desired. This concludes our proof of Theorem 20.2. □

Theorem 20.4. *(Eisenstein's criterion for irreducibility of polynomials) Let p be a prime number and let*

$$f(x) := \sum_{i=0}^{d} c_i x^i \in \mathbb{Z}[x]$$

be a polynomial satisfying the following properties:

(i) $p \nmid c_d$;
(ii) $p \mid c_i$ *for each* $i = 0, \dots, d-1$; *and*
(iii) $p^2 \nmid c_0$.

Then $f(x)$ must be irreducible.

Proof. As established in Theorem 20.2, it suffices to prove there exist no polynomials $g, h \in \mathbb{Z}[x]$ of degrees smaller than $d = \deg(f(x))$ such that $f(x) = g(x) \cdot h(x)$. We write

$$g(x) := \sum_{i=0}^{k} a_i x^i$$

for coefficients $a_i \in \mathbb{Z}$, and similarly,

$$h(x) := \sum_{j=0}^{\ell} b_j x^j.$$

We equate the coefficients c_i of $f(x)$ from using the fact that $f(x) = g(x) \cdot h(x)$; so, we obtain

$$c_0 = a_0 b_0 \text{ from the coefficient of the constant term in } f(x) \tag{127}$$

$$c_1 = a_0 b_1 + a_1 b_0 \text{ from the coefficient of } x \text{ in } f(x) \tag{128}$$

$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 \text{ from the coefficient of } x^2 \text{ in } f(x) \tag{129}$$

and so on, up to

$$c_d = a_k b_\ell \text{ from the coefficient of } x^{k+\ell} = x^d \text{ in } f(x). \tag{130}$$

Since $p \mid c_0 = a_0 b_0$, then we know that either a_0 or b_0 must be divisible by p. But since $p^2 \nmid c_0$ (by hypothesis (iii) in Theorem 20.4), then we know that precisely one of the two numbers a_0 or b_0 is divisible by p, while the other number is not divisble by p. So, without loss of generality, we assume

$$p \mid a_0 \text{ and } p \nmid b_0. \tag{131}$$

Using information (131) in (128), along with the fact that $p \mid c_1$, we get that

$$p \mid a_1. \tag{132}$$

Similarly, using that $p \mid c_2$ in (129) along with the information from (131) and (132), we get

$$p \mid a_2. \tag{133}$$

Claim 20.5. *With the above notation, $p \mid a_i$ for all $i = 0, \dots, k$.*

Proof of Claim 20.5. We prove $p \mid a_i$ by induction on i; we already covered above the first three cases for a_i. Now, if we know that $p \mid a_i$ for all $i < r$ (where $r \leq k$), next we show that also $p \mid a_r$.

Indeed, we have that the coefficient of x^r in $f(x) = g(x)h(x)$ must equal

$$c_r = \sum_{\substack{i+j=r \\ 0\leq i\leq k \\ 0\leq j\leq \ell}} a_i b_j = a_r b_0 + \sum_{\substack{i+j=r \\ 0\leq i< r \\ 1\leq j\leq \ell}} a_i b_j. \tag{134}$$

However, by our inductive hypothesis we have that $p \mid a_i$ for each $i = 0, \dots, r-1$. Also, $p \not| b_0$ (by (131)) and since $r \leq k$ and $k < d$, we also know by hypothesis (ii) in Theorem 20.4 that $p \mid c_r$. Combining all this information in (134), we obtain that indeed $p \mid a_r$.

This concludes our proof of Claim 20.5. □

So, Claim 20.5 yields that $p \mid a_k$ and thus, by (130), we conclude that $p \mid c_d$, which contradicts hypothesis (i) in Theorem 20.4. This means that indeed $f(x)$ must be irreducible. This concludes our proof of Theorem 20.4. □

A polynomial $f(x)$ satisfying the hypothesis (i)-(iii) in Theorem 20.4 is called a p-Eisenstein polynomial.

21. November 21

From now on, for the **odd prime number** p, we let ξ_p denote a *primitive* p-th root of unity, i.e., $\xi_p^p = 1$ but $\xi_p \neq 1$. To make things simpler, we can even fix the root of unity we consider, i.e.,

$$\xi_p = e^{\frac{2\pi i}{p}} = \cos\left(\frac{2\pi}{p}\right) + i \sin\left(\frac{2\pi}{p}\right).$$

Since $\xi_p^p - 1 = 0$ but $\xi_p - 1 \neq 0$, then ξ_p is a root of the polynomial

$$\Phi_p(x) := x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}. \tag{135}$$

We call Φ_p from (135), the *p-th cyclotomic polynomial.*

Proposition 21.1. *The p-th cyclotomic polynomial is irreducible.*

Proof. We have that $\Phi_p(x) = \frac{x^p-1}{x-1}$, which means that

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-2} + \binom{p}{2} x^{p-3} + \cdots + p.$$

Therefore, the polynomial $f(x) := \Phi_p(x+1)$ is a p-Eisenstein polynomial and so, $f(x)$ is irreducible. Now, if $\Phi_p(x)$ were reducible, then there would be some polynomials $g(x), h(x) \in \mathbb{Z}[x]$ of smaller degree than $p-1$ such that $\Phi_p(x) = g(x) \cdot h(x)$. But then also

$$f(x) = \Phi_p(x+1) = g(x+1) \cdot h(x+1),$$

and the polynomials $\tilde{g}(x) := g(x+1)$ and $\tilde{h}(x) := h(x+1)$ would have degree less than $\deg(f) = p-1$, contradicting the irreducibility of $f(x)$. So, $\Phi_p(x)$ is an irreducible polynomial, as desired. □

Proposition 21.2. *There exists no nonzero polynomial $f \in \mathbb{Q}[x]$ satisfying the following two properties:*

1. *$f(\xi_p) = 0$; and*
2. *$\deg(f) < p-1$.*

Proof. We argue by contradiction and therefore assume there exists some nonzero polynomial $f(x)$ satisfying the conditions (1)-(2) above. Furthermore, we pick such a polynomial $f(x)$ of minimum degree; say $d := \deg(f) < p-1$. Also, $d > 0$ because f cannot be a nonzero constant polynomial and still vanish at ξ_p.

Now, we divide $\Phi_p(x)$ by $f(x)$ and obtain quotient $Q(x)$ and remainder $R(x)$, i.e.,

$$\Phi_p(x) = f(x)Q(x) + R(x), \tag{136}$$

where $\deg(R) < \deg(f) = d$. Using that both $\Phi_p(\xi_p) = 0$ and $f(\xi_p) = 0$ in (136), we conclude that also $R(\xi_p) = 0$. Also, due to the long division algorithm for polynomials, we have that $R \in \mathbb{Q}[x]$. So, if $R(x)$ were a nonzero polynomial, then we would have a polynomial $R(x)$ satisfying conditions (1)-(2) above and have smaller degree than $f(x)$ (which has the *smallest* degree among such polynomials). Thus, we have $R(x) = 0$, i.e.,

$$\Phi_p(x) = f(x)Q(x),$$

which contradicts the irreducibility of the p-th cyclotomic polynomial (established in Poposition 21.1); note that $0 < \deg(f) < p-1$, which means that also $0 < \deg(Q) < p-1$. So, indeed, there exists no nonzero polynomial $f(x)$ satisfying conditions (1)-(2) above. This concludes our proof of Proposition 21.2. □

Corollary 21.3. *Let $a_1, \dots, a_{p-1}, b_1, \dots, b_{p-1} \in \mathbb{Z}$ such that*

$$\sum_{i=1}^{p-1} a_i \xi_p^i = \sum_{i=1}^{p-1} b_i \xi_p^i.$$

Then we must have that $a_i = b_i$ for each $i = 1, \dots, p-1$.

Proof. Let $f(x)$ be the polynomial with integer coefficients:

$$f(x) := (a_1 - b_1) + (a_2 - b_2)x + (a_3 - b_3)x^2 + \cdots + (a_{p-1} - b_{p-1})x^{p-2}.$$

Then $f(\xi_p) = 0$ and since $\deg(f) < p-1$, Proposition 21.2 forces that $f(x) = 0$, i.e., $a_i = b_i$ for each $i = 1, \dots, p-1$. □

Proposition 21.4. *Let $b \in \mathbb{Z}$. Then*

$$\sum_{i=1}^{p-1} \xi_p^{bi} = \begin{cases} -1 & \text{if} \quad p \not| b \\ p-1 & \text{if} \quad p \mid b \end{cases}$$

Proof. If $p \mid b$, then $p \mid bi$ for each $i = 1, \dots, p-1$, which means that indeed,

$$\sum_{i=1}^{p-1} \xi_p^{bi} = \sum_{i=1}^{p-1} 1 = p - 1.$$

Now, if $p \not| b$, then b is invertible modulo p and therefore multiplying by b the complete set of nonzero residue classes

$$\{1, 2, \dots, p-1\}$$

induces a bijection on this set (this is the same argument employed in the proof of Theorem 10.2). So, since ξ_p is a p-th root of unity, then the sum $\sum_{i=1}^{p-1} \xi_p^{bi}$ is the same as the sum $\sum_{i=1}^{p-1} \xi_p^i$. However, since

$$1 + \xi_p + \xi_p^2 + \cdots + \xi_p^{p-1} = 0,$$

we conclude that indeed, $\sum_{i=1}^{p-1} \xi_p^{bi} = -1$ if $p \not| b$. □

Proposition 21.5. *Let p be a prime number, let $n \in \mathbb{N}$ and let $x_1, \dots, x_n$ be arbitrary variables. Then the coefficient of each monomial in*

$$\left(\sum_{i=1}^{n}\right)^p - \sum_{i=1}^{n} x_i^p \tag{137}$$

is divisible by p.

Proof. We prove the result by induction on n; the case $n = 2$ is simply the binomial expansion and in this case, we know that for each $i = 1, \dots, p-1$, we have that $p \mid \binom{p}{i}$. So, we assume the result holds for some integer $n \geq 2$ and we prove it for $n+1$. Then we write

$$\left(\sum_{i=1}^{n+1} x_i\right)^p - \sum_{i=1}^{n+1} x_i^p \tag{138}$$

as

$$((x_1 + x_2) + x_3 + x_4 + \cdots + x_n + x_{n+1})^p - (x_1+x_2)^p - x_3^p - x_4^p - \cdots - x_{n-1}^p - x_n^p + \sum_{i=1}^{p-1} \binom{p}{i} x_1^i x_2^{p-i}$$

and applying the inductive hypothesis for the n variables $(x_1+x_2), x_3, x_4, \dots, x_n, x_{n+1}$, we get that indeed each coefficient in the expansion from (138) must be divisible by p, as claimed in Proposition 21.5. □

Proposition 21.6. *Let p be a prime number, let $m, n \in \mathbb{N}$, let $i_1, \dots, i_n$ and $c_1, \dots, c_n$ be integers with the property that m divides each c_j for $j = 1, \dots, n$. Then there exist integers $b_1, \dots, b_{p-1}$ all divisible by m such that*

$$\sum_{j=1}^{n} c_j \xi_p^{i_j} = \sum_{j=1}^{p-1} b_j \xi_p^j. \tag{139}$$

Proof. First of all, we let for each $\ell = 0, \dots, p-1$:

$$a_\ell = \sum_{\substack{1 \leq j \leq n \\ i_j \equiv \ell \pmod p}} c_j;$$

so then

$$\sum_{j=1}^{n} c_j \xi_p^{i_j} = \sum_{\ell=0}^{p-1} a_\ell \xi_p^\ell. \tag{140}$$

Clearly, $m \mid a_\ell$ for each $\ell = 0, \dots, p-1$. Using the fact that

$$1 = -\xi_p - \xi_p^2 - \cdots - \xi_p^{p-1},$$

then letting for each $j = 1, \dots, p-1$:

$$b_j = a_j - a_0,$$

we conclude that (139) holds, i.e.,

$$\sum_{j=1}^{n} c_j \xi_p^{i_j} = \sum_{j=1}^{p-1} b_j \xi_p^j.$$

Furthermore, $m \mid b_j$ for each $j = 1, \dots, p-1$, as claimed in Proposition 21.6. □

22. November 23

Definition 22.1. *Let p be an odd prime number. We define the Gauss sum to be*

$$G(p) := \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \cdot \xi_p^i.$$

For example, we have

$$G(3) = \xi_3 - \xi_3^2;$$
$$G(5) = \xi_5 - \xi_5^2 - \xi_5^3 + \xi_5^4;$$
$$G(7) = \xi_7 + \xi_7^2 - \xi_7^3 + \xi_7^4 - \xi_7^5 - \xi_7^6.$$

Theorem 22.2. *With the above notation for the Gauss sum, we have*

$$G(p)^2 = p \cdot \left(\frac{-1}{p}\right) = p \cdot (-1)^{\frac{p-1}{2}}. \tag{141}$$

Proof of Theorem 22.2. We compute

$$\begin{aligned} &G(p)^2 \\ &= \left(\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \xi_p^i\right) \cdot \left(\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \xi_p^j\right) \\ &= \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \xi_p^i \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \xi_p^j. \end{aligned}$$

The crucial observation is that for the inner sum above, for each fixed $i = 1, \dots, p-1$, if we replace j by $j \cdot i$ in that inner sum, the sum won't change simply because both the Legendre symbol and also the powers of ξ_p only depend on the residue classes of j (respectively ji) modulo p, i.e., we're simply using that

$$\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \cdot \xi_p^j = \sum_{j=1}^{p-1} \left(\frac{ij}{p}\right) \cdot \xi_p^{ij},$$

because the second sum above is simply a re-writing of the first sum where the order of the terms was shuffled around because

$$\{1, 2, \ldots, p-1\} \text{ modulo } p \text{ is the same as } \{i, 2i, \ldots, i(p-1)\} \text{ modulo } p,$$

as i is invertible modulo p for each $i = 1, \ldots, p-1$. So,

$$\begin{aligned} &G(p)^2 \\ &= \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \xi_p^i \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \xi_p^j \\ &= \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \xi_p^i \sum_{j=1}^{p-1} \left(\frac{ij}{p}\right) \xi_p^{ij} \\ &= \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} \left(\frac{i^2 j}{p}\right) \xi_p^{ij+i} \\ &= \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \xi_p^{i(j+1)} \\ &= \sum_{j=1}^{p-1} \sum_{i=1}^{p-1} \left(\frac{j}{p}\right) \xi_p^{(j+1)i} \\ &= \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \cdot \sum_{i=1}^{p-1} \xi_p^{(j+1)i}. \end{aligned}$$

Now, according to Proposition 21.4, we have that

$$\sum_{i=1}^{p-1} \xi_p^{(j+1)i} = \begin{cases} p-1 & \text{if} \quad j = p-1 \\ -1 & \text{if} \quad j = 1, \ldots, p-2 \end{cases}$$

Using this computation in the inner sum above, we compute

$$\begin{aligned} &G(p)^2 \\ &= \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \cdot \sum_{i=1}^{p-1} \xi_p^{(j+1)i} \\ &= \left(\frac{p-1}{p}\right) \cdot (p-1) - \sum_{j=1}^{p-2} \left(\frac{j}{p}\right). \end{aligned}$$

However, according to Proposition 19.4, we have

$$-\sum_{j=1}^{p-2} \left(\frac{j}{p}\right) = \left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right).$$

Finally, using this last information in the above summation for $G(p)^2$ yields the desired formula:

$$G(p)^2 = p \left(\frac{-1}{p}\right),$$

as claimed in the conclusion of Theorem 22.2. □

Proof of Theorem 19.7. We compute $G(p)^q$ in two different ways. First of all, using Theorem 22.2, we have

$$G(p)^q = G(p)\cdot G(p)^{q-1} = G(p)\cdot \left(G(p)^2\right)^{\frac{q-1}{2}} = G(p)\cdot\left(p\left(\frac{-1}{p}\right)\right)^{\frac{q-1}{2}}. \tag{142}$$

Now, according to property (ii) of Proposition 19.3, we have $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, which allows us to conclude (note also the definition of the Gauss sum $G(p)$) that

$$G(p)^q = (-1)^{\frac{(p-1)(q-1)}{4}}\cdot p^{\frac{q-1}{2}}\cdot\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\xi_p^i. \tag{143}$$

Applying Proposition 19.2, we get

$$p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) \pmod{q}, \tag{144}$$

which, in particular, it means that there exists an integer k such that

$$p^{\frac{q-1}{2}} - \left(\frac{p}{q}\right) = kq. \tag{145}$$

Using (145) in (143) yields the existence of some integers $a_1,\dots,a_{p-1}$, each one of them divisible by q such that

$$G(p)^q = (-1)^{\frac{(p-1)(q-1)}{4}}\cdot\left(\frac{p}{q}\right)\cdot G(p) + \sum_{i=1}^{p-1}a_i\xi_p^i. \tag{146}$$

Next we compute $G(p)^q$ in a different way, using Proposition 21.5. So,

$$G(p)^q = \left(\left(\frac{1}{p}\right)\xi_p + \left(\frac{2}{p}\right)\xi_p^2 + \cdots + \left(\frac{p-1}{p}\right)\xi_p^{p-1}\right)^q$$

and then invoking Proposition 21.5, we get the existence of some integers i_j (for $j=1,\dots,n$, where n is some positive integer) and also, the existence of some integers c_j with $q\mid c_j$ (for each $j=1,\dots,n$) such that

$$G(p)^q = \sum_{i=1}^{p-1}\left(\left(\frac{i}{p}\right)\xi_p^i\right)^q + \sum_{j=1}^{n}c_j\xi_p^{i_j}. \tag{147}$$

Using Proposition 21.6 allows us to re-write the above sum as follows:

$$G(p)^q = \sum_{i=1}^{p-1}\left(\left(\frac{i}{p}\right)\xi_p^i\right)^q + \sum_{j=1}^{p-1}b_j\xi_p^j, \tag{148}$$

for some integers b_j, each one of them divisible by q. Finally, we simplify the above sum using that $\left(\frac{i}{p}\right)^q = \left(\frac{i}{p}\right)$ for each $i=1,\dots,p-1$ (since q is odd):

$$G(p)^q = \sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\xi_p^{iq} + \sum_{j=1}^{p-1}b_j\xi_p^j. \tag{149}$$

Now, using property (i) from Proposition 19.3, we have

$$\left(\frac{i}{q}\right) = \left(\frac{iq^2}{p}\right) \text{ for each } i=1,\dots,p-1$$

and so, we compute:

$$\begin{aligned}
&G(p)^q\\
&\quad=\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\xi_p^{iq}+\sum_{j=1}^{p-1}b_j\xi_p^j\\
&\quad=\sum_{i=1}^{p-1}\left(\frac{iq^2}{p}\right)\xi_p^{iq}+\sum_{j=1}^{p-1}b_j\xi_p^j\\
&\quad=\sum_{i=1}^{p-1}\left(\frac{q}{p}\right)\cdot\left(\frac{iq}{p}\right)\xi_p^{iq}+\sum_{j=1}^{p-1}b_j\xi_p^j\\
&\quad=\left(\frac{q}{p}\right)\cdot\sum_{i=1}^{p-1}\left(\frac{iq}{p}\right)\xi_p^{iq}+\sum_{j=1}^{p-1}b_j\xi_p^j\\
&\quad\left(\frac{q}{p}\right)\cdot\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\xi_p^{i}+\sum_{j=1}^{p-1}b_j\xi_p^j,
\end{aligned}$$

where in the last formula, we used again the observation from the beginning of our proof that a Gauss sum is unchanged when we shuffle around the terms according (in this latter application) to

$$\{q,2q,\dots,q(p-1)\}\text{ modulo }p\text{ is the same as }\{1,2,\dots,p-1\}\text{ modulo }p.$$

Therefore,

$$G(p)^q=\left(\frac{q}{p}\right)\cdot G(p)+\sum_{j=1}^{p-1}b_j\xi_p^j. \tag{150}$$

Then letting $d_j := b_j - a_j$ for $j = 1, \dots, p-1$, we get (after comparing equations (150) and (146)) that

$$\left((-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)-\left(\frac{q}{p}\right)\right)\cdot G(p)=\sum_{j=1}^{p-1}d_j\xi_p^j. \tag{151}$$

Using now Corollary 21.3 (since $G(p)$ is itself a linear combination of $\xi_p, \xi_p^2, \cdots, \xi_p^{p-1}$ with integer coefficients), we obtain that the coefficient of ξ_p^j (for $j = 1, \dots, p-1$) from the right-hand side of equation (151) must match the coefficient of ξ_p^j appearing in the left-hand side of the same equation above. In other words, comparing the coefficients of ξ_p in both sides of (151), we get that

$$\left((-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)-\left(\frac{q}{p}\right)\right)\cdot\left(\frac{1}{p}\right)=d_1. \tag{152}$$

Now, since d_1 is divisible by q (because both b_1 and c_1 are divisible by q), combining with the fact that $\left(\frac{1}{p}\right) = 1$ along with the fact that

$$\left((-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)-\left(\frac{q}{p}\right)\right)\in\{-2,0,2\},$$

allows us to conclude that indeed,

$$(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)-\left(\frac{q}{p}\right)=0. \tag{153}$$

In particular, we established the Gauss Quadratic Reciprocity Law. □

23. November 28

Definition 23.1. *A Diophantine equation is an equation of the form*

$$f(x_1,\dots,x_n)=0, \tag{154}$$

where f is a polynomial in n variables (for some integer $n\ge 2$) whose coefficients are all integers, and furthermore, we are interested in solving the equation (154) over the integers.

Typical examples of Diophantine equations are the Fermat's equations:

$$x^2+y^2=z^2, \tag{155}$$

for which we will find all solutions (there exist infinitely many nonzero integer solutions to (155), as proven in Proposition 23.6), but also

$$x^4+y^4=z^4, \tag{156}$$

for which there exist no nonzero integer solutions (as we will prove in Theorem 23.7), and more generally,

$$x^n+y^n=z^n, \tag{157}$$

for any given integer $n\ge 3$, in which case, again there exist no integer nonzero integer solutions (i.e., any integer solutions (x,y,z) to either equation (156) or more generally, to equation (157) must satisfy $x\cdot y\cdot z=0$). However, proving this last statement about the general equation (157) is **way beyond** the scope of our current course.

Proposition 23.2. *Let $a,b\in\mathbb{Z}$ and let $n\in\mathbb{N}$. If $a^n\mid b^n$, then $a\mid b$.*

Proof. Let $d=\gcd(a,b)$; our goal is to prove $d=|a|$ (note that a may be negative) since this will show that $a\mid b$.

Now, if $d\ne|a|$, then that means actually that $d<|a|$ (note that d is a divisor of $|a|$). So, in this case, letting

$$a_1:=\frac{a}{d}\text{ and }b_1=\frac{b}{d},$$

we have that $|a_1|>1$ and also, $\gcd(a_1,b_1)=1$. Furthermore, the divisibility $a^n\mid b^n$ is equivalent (after dividing both sides by d^n which is a divisor of both) with $a_1^n\mid b_1^n$. However, $\gcd(a_1,b_1)=1$, which also implies $\gcd(a_1^n,b_1^n)=1$, contradicting thus the divisibility $a_1^n\mid b_1^n$ because $|a_1|>1$ (and therefore contradicting the divisibility $a^n\mid b^n$). So, we must have $d=|a|$, i.e., $a\mid b$, as claimed in Proposition 23.2. □

Proposition 23.3. *Let $k,n\in\mathbb{N}$ and let $a_1,\dots,a_n\in\mathbb{N}$, which are pairwise coprime. If there exists $b\in\mathbb{N}$ such that*

$$\prod_{i=1}^{n}a_i=b^k. \tag{158}$$

Then there exist $b_i\in\mathbb{N}$ such that for each $i=1,\dots,n$, we have $a_i=b_i^k$.

Proof. Using equation (158), we get that for each prime number p, the exponent of p in b^k and therefore in the product $\prod_{i=1}^n a_i$ is divisible by k. However, the numbers a_i are coprime which means that for each prime p, the exponent of p in a_i is either 0 or it equals a positive integer divisible by k. So, every single exponent of a prime appearing in the prime power factorization of each number a_i must be divisible by k; so, a_i is a perfect k-th power, exactly as claimed in the conclusion of Proposition 23.3. □

Proposition 23.4. *Let $a, b, c \in \mathbb{Z}$, not all equal to 0, such that $a^2 + b^2 = c^2$. Then*

$$\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = \gcd(a, b, c). \tag{159}$$

Proof. First of all, since not all of the integers a, b, c can be 0, then actually at most one of them (either a or b) may equal 0.

Let $d = \gcd(a, b)$; then $d^2 \mid a^2 + b^2$ and so, $d^2 \mid c^2$. Then Proposition 23.2 yields $d \mid c$. Therefore, $\gcd(a, b) = \gcd(a, b, c)$ (note that automatically, $\gcd(a, b, c) \le \gcd(a, b)$ but then our argument proves the reverse inequality as well).

Similarly, letting $e := \gcd(a, c)$, then $e^2 \mid c^2 - a^2$ and so, $e^2 \mid b^2$ and once again, Proposition 23.2 yields $e \mid b$ and in turn, $\gcd(a, c) = \gcd(a, b, c)$.

Finally, the exact same argument as above yields that if $f = \gcd(b, c)$, then $f \mid a$ as well. So, indeed

$$\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = \gcd(a, b, c),$$

as claimed in Proposition 23.4. □

Proposition 23.4 shows that for any solution $(a, b, c) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$ to the equation (155), we can divide by the common greatest common divisor d of the three numbers a, b, c, and then the corresponding integers from this outcome:

$$a_1 := \frac{a}{d},\ b_1 := \frac{b}{d} \text{ and } c_1 := \frac{c}{d}$$

are now pairwise coprime, i.e,

$$\gcd(a_1, b_1) = \gcd(a_1, c_1) = \gcd(b_1, c_1) = \gcd(a_1, b_1, c_1) = 1.$$

Furthermore, since $a^2 + b^2 = c^2$, then dividing by d^2 this last equality yields that also (a_1, b_1, c_1) are solutions to equation (155). Therefore, it means that when solving the equation (155), we can always reduce (at the expense of dividing any solutions a, b, c by their greatest common divisor) that the solutions we found to the equation (155) are pairwise coprime. This justifies the following findings:

Proposition 23.5. *Let $a, b, c \in \mathbb{Z}$ such that $a^2 + b^2 = c^2$ and furthermore, assume* $\gcd(a, b, c) = 1$. *Then c must be odd and precisely one of the two numbers a or b must also be odd, while the other number must be even.*

Proof. Clearly, we cannot have two of the three numbers a, b or c even, since we're assuming $\gcd(a, b, c) = 1$ and in Proposition 23.4 we already proved that

$$\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = \gcd(a, b, c) = 1$$

in our case. Now, solely based on parity analysis, we cannot have all three integers a, b and c odd; therefore, precisely one of these three numbers is even, while the other two integers are odd. So, the only thing remaining to be shown is that we cannot have that c is even while both a and b are odd.

Now, if both a and b are odd, then

$$a^2 \equiv b^2 \equiv 1 \pmod{4}$$

and so, we would have that $c^2 \equiv 2 \pmod{4}$, which is impossible because the square of an even integer must be divisible by 4. This contradiction proves that indeed, c must be odd and precisely one of the two numbers a or b must also be odd, while the other number must be even. □

Therefore, when solving for all the Pythagorean triples, i.e., integers a, b, c satisfying equation (155), we may always assume that

$$\gcd(a, b, c) = 1$$

and furthermore, without loss of generality, we may assume a is even, while b and c are odd.

Proposition 23.6. *(Pythagorean triples) Let $a, b, c \in \mathbb{N}$ such that*

1. *$a^2 + b^2 = c^2$;*
2. *$\gcd(a, b, c) = 1$; and*
3. *a is even, while b and c are odd.*

Then there exist coprime positive integers $s > t$, not both of them odd, such that

$$a = 2st,\ b = s^2 - t^2 \text{ and } c = s^2 + t^2.$$

Proof. We have $a^2 = (c - b)(c + b)$. By our hypothesis, both $c - b$ and $c + b$ are even positive integers; so, we write

$$s - b = 2T \text{ and } c + b = 2S,$$

for some positive integers S and T. Since a is even, we write $a = 2A$ for some positive integer A and then we get

$$A^2 = ST. \tag{160}$$

Since $\gcd(b, c) = 1$, then $\gcd(S, T) = 1$ (since any prime factor of S and T would then be a prime factor of both c and b as $c = S + T$ and $b = S - T$). But then using that $\gcd(S, T) = 1$ in (160), combined with Proposition 23.3 yields that both S and T must be perfect squares, i.e,

$$S = s^2 \text{ and } T = t^2$$

for some coprime positive integers s and t. Using this last information in equation (160) yields that $A = st$ and therefore, $a = 2st$. Finally, because $b = S - T$ and $c = S + T$, we derive the desired formulas for a, b, c, as claimed in the conclusion of Proposition 23.6. □

Theorem 23.7. *(Fermat's Last Theorem for $n = 4$) There exist no positive integer solutions to the Diophantine equation:*

$$x^4 + y^4 = z^4. \tag{161}$$

Proof. We will prove the even stronger statement that there exist no solutions in positive integers to the equation

$$x^4 + y^4 = z^2. \tag{162}$$

In order to achieve our goal, we argue by contradiction and therefore, assume there exist solutions in $\mathbb{N}^3$ to equation (162); so, we pick $x_0, y_0, z_0 \in \mathbb{N}$ solutions to equation (162) which minimize z_0 among any such solutions.

Claim 23.8. *With the above notation,* $\gcd(x_0, y_0) = 1$.

Proof of Claim 23.8. If there exists a prime number q dividing both x_0 and y_0, then

$$q^4 \mid (x_0^4 + y_0^4) = z_0^2.$$

But then Proposition 23.2 yields that $q^2 \mid z_0$. So, then we note that the positive integers

$$x_1 := \frac{x_0}{q},\ y_1 := \frac{y_0}{q} \text{ and } z_1 := \frac{z_0}{q^2}$$

are solutions to the equation (162) and furthermore, $z_1 < z_0$, contradicting thus the minimality of z_0. Therefore, we must have that $\gcd(x_0, y_0) = 1$, as desired in the conclusion of Claim 23.8. □

Using Claim 23.8 along with Proposition 23.4, we conclude that the positive integers x_0, y_0 and z_0 must be coprime since

$$\left(x_0^2\right)^2 + \left(y_0^2\right)^2 = z_0^2. \tag{163}$$

In particular, then using Proposition 23.5, we may assume (without loss of generality) that x_0 is even and y_0 is odd, while z_0 must be odd. Then Proposition 23.6 yields the existence of coprime positive integers $s > t$ such that

$$x_0^2 = 2st,\ y_0^2 = s^2 - t^2 \text{ and } z_0 = s^2 + t^2. \tag{164}$$

In particular, we must have

$$s^2 = y_0^2 + t^2$$

and since $\gcd(s, t) = 1$, then once again applying Proposition 23.5, we conclude that s must be odd. Furthermore, since we have that y_0 is odd, then we must have that t is even; so, we can write

$$t := 2u$$

for some positive integer u. Now, using that $t = 2u$ along with the fact that x_0 is even (and so, we can write $x_0 := 2x_1$ for some $x_1 \in \mathbb{N}$) in the relation

$$x_0^2 = 2st \text{ (coming from (164))},$$

we get that

$$x_1^2 = su. \tag{165}$$

Furthermore, because $\gcd(s, t) = 1$ and $t = 2u$, then we also have that $\gcd(s, u) = 1$. Using this relation in equation (165), then Proposition 23.3 yields the existence of positive integers v and w such that

$$s = v^2,\ u = w^2 \text{ and } x_1 = vw. \tag{166}$$

So,

$$t = 2w^2 \text{ and } s = v^2. \tag{167}$$

Next we turn our attention to the relation (coming from (164))

$$s^2 = y_0^2 + t^2. \tag{168}$$

We know that the positive integers s, y_0, t are coprime and moreover, t is even; so, Proposition 23.6 yields the existence of coprime positive integers $a > b$ such that

$$t = 2ab,\ y_0 = a^2 - b^2 \text{ and } s = a^2 + b^2. \tag{169}$$

However, $t = 2w^2$, which combined with the formula from (169) yields

$$w^2 = ab. \tag{170}$$

Using that $\gcd(a, b) = 1$ in equation (170), then Proposition 23.3 yields the existence of positive integers c and d such that

$$a = c^2,\ b = d^2 \text{ and } w = cd. \tag{171}$$

So, using the formulas for a and b in (171) in the last formula from the equations in (169), we get that

$$c^4 + d^4 = s. \tag{172}$$

Finally, using that $s = v^2$ (which is first formula in (166)), we get

$$c^4 + d^4 = v^2. \tag{173}$$

So, c, d, v are also positive integer solutions to the equation (162). However, we see that

$$v \le x_1 = vw \text{ (from (166))}. \tag{174}$$

On the other hand,

$$x_1 < 2x_1 = x_0 \le x_0^2 < z_0 \text{ because } x_0^4 + y_0^4 = z_0^2. \tag{175}$$

Combining (174) and (175), we get that $v < z_0$, which therefore contradicts the minimality of z_0. This contradiction proves that there does not exist solutions in $\mathbb{N}^3$ to the Diophantine equation (162) ad so, there exist no solutions in $\mathbb{N}^3$ to Fermat's equation with exponent 4.

This concludes our proof of Theorem 23.7. □

24. December 5

Proposition 24.1. *Let $d \in \mathbb{N}$. Then $\sqrt{d} \in \mathbb{N}$ if and only if $\sqrt{d} \in \mathbb{Q}$.*

Proof. Clearly, if $\sqrt{d} \in \mathbb{N}$, then $\sqrt{d} \in \mathbb{Q}$. Now, for the converse, assume there exist coprime positive integers (after all, $\sqrt{d} > 0$) such that

$$\sqrt{d} = \frac{a}{b}.$$

But then $b^2 d = a^2$; so, $b^2 \mid a^2$ and Proposition 23.2 yields that $b \mid a$. But $\gcd(a, b) = 1$, which means that $b = 1$; hence $d = a^2$ which means that $\sqrt{d} = a \in \mathbb{N}$, as desired for the conclusion of Proposition 24.1. □

Theorem 24.2. *(Pell's equation) Let $d \in \mathbb{N}$ such that $\sqrt{d} \notin \mathbb{N}$. Then there exist infinitely many positive integers x and y such that*

$$x^2 - dy^2 = 1. \tag{176}$$

Proof. First of all, we note that once there exists **one** solution $(x_1, y_1) \in \mathbb{N}^2$ for the equation (176), then we can construct infinitely many solutions to the Pell's equation. Indeed, for any two solutions in $\mathbb{N}^2$ to (176) (say, (x_1, y_1) and (x_2, y_2), not necessarily distinct such pairs) then we can construct a third solution (x_3, y_3) for which

$$x_3 > \max\{x_1, x_2\} \text{ and } y_3 > \max\{y_1, y_2\}, \tag{177}$$

thus proving that (x_3, y_3) is indeed a new solution to equation (176) (different than (x_1, y_1) and (x_2, y_2)). The key for us will be the identity:

$$(x_1^2 - dy_1^2) \cdot (x_2^2 - dy_2^2) = (x_1x_2 + dy_1y_2)^2 - d(x_1y_2 + x_2y_1)^2. \tag{178}$$

So, if (x_1, y_1) and (x_2, y_2) are solutions to equation (176), then

$$x_3 = x_1x_2 + dy_1y_2 \text{ and } y_3 = x_1y_2 + x_2y_1$$

is a solution to (176) and clearly, inequalities (177) are satisfied, thus proving that (x_3, y_3) is indeed a new solution to the Pell's equation. Therefore, once we have just *one* solution in positive integers to equation (176), then we actually get infinitely many such solutions. Thus, from now on, we will focus on proving the existence of one solution in positive integers to equation (176).

In order to achieve our goal, we will prove in the process several very useful results beyond their application to the Pell's equation; moreover, these results are meaningful for *Diophantine apporximation*, i.e., how well we can approximate an irrational number through rationals.

Proposition 24.3. *Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and let $N \in \mathbb{N}$. Then there exists an integer p and a positive integer $q \le N$ such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qN}. \tag{179}$$

Proof of Proposition 24.3. We recall the notation $\{z\}$ for the frational part of the real number z, which is defined to be $z - [z]$, where $[z]$ is the integer part of z, i.e., the largest integer less than or equal to z. Therefore, always $0 \le \{z\} < 1$.

We consider all the fractional parts $\{i \cdot \alpha\}$ for $0 \le i \le N$. Since we have $N + 1$ such numbers in the interval $[0, 1)$, we conclude (by the Pigeonhole Principle) that there must exist

$$0 \le i < j \le N \tag{180}$$

such that

$$|\{j\alpha\} - \{i\alpha\}| < \frac{1}{N}. \tag{181}$$

We write $\{j\alpha\} = j\alpha - [j\alpha]$ and $\{i\alpha\} = i\alpha - [i\alpha]$ and so, inequality (181) becomes

$$|j\alpha - [j\alpha] - i\alpha + [i\alpha]| < \frac{1}{N}. \tag{182}$$

Letting $q := j - i$ and $p := [j\alpha] - [i\alpha]$, we have clearly $1 \le q \le N$ (as desired in the conclusion of Proposition 24.3) and

$$|q\alpha - p| < \frac{1}{N}$$

and so,

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qN},$$

which concludes our proof of Proposition 24.3. □

Corollary 24.4. *Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Then there exist infinitely many distinct pairs $(p, q) \in \mathbb{Z} \times \mathbb{N}$ such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{183}$$

Proof of Corollary 24.4. By Proposition 24.3, we know that for each $N \in \mathbb{N}$, there exists a pair $(p_N, q_N) \in \mathbb{Z} \times \mathbb{N}$ such that

(i) $\left|\alpha - \frac{p_N}{q_N}\right| < \frac{1}{q_N \cdot N}$, and
(ii) $q_N \le N$.

Combining (i) and (ii), we obtain

$$\left|\alpha - \frac{p_N}{q_N}\right| < \frac{1}{q_N^2}. \tag{184}$$

So, in order to obtain the desired conclusion in Corollary 24.4, all we need to guarantee is that there exist infinitely mnay distinct pairs among the sequence of all pairs $\{(p_N, q_N)\}_{N\in\mathbb{N}}$.

Now, if there were only finitely many pairs among the above sequence of pairs, then (by the Pigeonhole Principle) it means that there exists a certain pair $(p, q) \in \mathbb{Z} \times \mathbb{N}$ such that

$$(p_N, q_N) = (p, q) \text{ for infinitely many } N \in \mathbb{N}.$$

But then inequality (i) applied to each one of the pairs $(p_N, q_N) = (p, q)$ would yield

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q_N \cdot N} \le \frac{1}{N}. \tag{185}$$

However, if inequality (185) were to hold for infinitely mnay $N \in \mathbb{N}$, then it means that actually $\alpha = \frac{p}{q}$, contradicting the fact that $\alpha \notin \mathbb{Q}$. Thus, indeed, there must exist infinitely many distinct pairs in the sequence of pairs $\{(p_N, q_N)\}_{N\in\mathbb{N}}$; since for each such pair, we have the inequality (184), we obtain the desired conclusion in Corollary 24.4. □

We apply the above findings to the irrational number $\sqrt{d}$ (note also Proposition 24.1) and obtain the following result.

Proposition 24.5. *There exist a nonzero integer D and there exist infinitely many distinct pairs $(a, b) \in \mathbb{N}^2$ with the property that*

$$a^2 - db^2 = D. \tag{186}$$

Proof of Proposition 24.5. Since $\sqrt{d} \notin \mathbb{Q}$, then according to Corollary 24.4, there exist infinitely many pairs $(p_n, q_n) \in \mathbb{Z} \times \mathbb{N}$ such that

$$\left|\sqrt{d} - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}. \tag{187}$$

In particular, $p_n \in \mathbb{N}$ since otherwise the left-hand side in inequality (187) would be larger than $1 \ge \frac{1}{q_n^2}$, contradiction.

Now, for each $n \in \mathbb{N}$, inequality (187) yields

$$\left|\frac{p_n}{q_n} + \sqrt{d}\right| = \frac{p_n}{q_n} + \sqrt{d} = 2\sqrt{d} + \left(\frac{p_n}{q_n} - \sqrt{d}\right) < 2\sqrt{d} + 1$$

and so,

$$\begin{aligned} &\left|p_n^2 - dq_n^2\right| \\ = &\left|p_n - \sqrt{d}q_n\right| \cdot \left(p_n + \sqrt{d}q_n\right) \\ = &q_n^2 \cdot \left|\frac{p_n}{q_n} - \sqrt{d}\right| \cdot \left(\frac{p_n}{q_n} + \sqrt{d}\right) \\ < &q_n^2 \cdot \frac{1}{q_n^2} \cdot \left(2\sqrt{d} + 1\right) \\ = &2\sqrt{d} + 1. \end{aligned}$$

So, by the Pigeonhole Principle, there exists some integer D such that for infinitely many (distinct) pairs $(p_n, q_n) \in \mathbb{N}^2$, we have

$$p_n^2 - dq_n^2 = D.$$

Finally, $D \neq 0$ since otherwise we would have that $\sqrt{d} = \frac{p_n}{q_n}$, contradiction. This concludes our proof of Proposition 24.5. □

Now, let D be as in the conclusion of Proposition 24.5. Since there exist infinitely many pairs of positive integers a and b satisfying the equation (186), then by the Pigeonhole Principle, we can find two (distinct) pairs (a_1, b_1) and (a_2, b_2) satisfying both equation (186) and also,

$$a_2 \equiv a_1 \pmod{D} \text{ and } b_2 \equiv b_1 \pmod{D}. \tag{188}$$

Next we use the identity:

$$(A_1^2 - dB_1^2)(A_2^2 - dB_2^2) = (A_1A_2 - dB_1B_2)^2 - d(A_1B_2 - A_2B_1)^2. \tag{189}$$

Now, we observe that (using (188)) we have

$$a_1b_2 - a_2b_1 \equiv a_1b_1 - a_1b_1 \equiv 0 \pmod{D} \text{ and}$$
$$a_1a_2 - db_1b_2 \equiv a_1^2 - db_1^2 \equiv D \equiv 0 \pmod{D}.$$

So, we let the nonnegative integers:

$$x_0 := \left|\frac{a_1a_2 - db_1b_2}{D}\right| \text{ and } y_0 := \left|\frac{a_1b_2 - a_2b_1}{D}\right|.$$

Using identity (189), we see that

$$x_0^2 - dy_0^2 = 1. \tag{190}$$

So, all is left for us to check is that the solution (x_0, y_0) to the Pell's equation (190) is not the *trivial* solution $(1, 0)$; note that already we know that $x_0, y_0 \geq 0$.

Now, if $y_0 = 0$, then we would have that $a_2b_1 = a_1b_2$ and since the numbers a_i and b_i are positive, then we would have that there exists a positive rational number r such that

$$r := \frac{a_2}{a_1} = \frac{b_2}{b_1}.$$

But then we would have:

$$D = a_2^2 - db_2^2 = r^2 \cdot (a_1^2 - db_1^2) = r^2 \cdot D$$

and so, $r = 1$. But then this would mean that actually $(a_1, b_1) = (a_2, b_2)$, contradicting the fact that the two pairs of solutions to equation (186) are distinct. So, indeed, $y_0 > 0$, i.e., $(x_0, y_0) \in \mathbb{N}^2$ is a nontrivial solution to Pell's equation (176). This concludes our proof of Theorem 24.2. □

Proposition 24.6. *Let $d \in \mathbb{N}$ such that $\sqrt{d} \notin \mathbb{N}$ and let $(x_1, y_1) \in \mathbb{N}^2$ be a solution to the equation*

$$x^2 - dy^2 = 1 \tag{191}$$

with the property that y_1 is minimal among all solutions in positive integers to the equation (191). Then for any solution $(x, y) \in \mathbb{N}^2$ to the equation (191), there must exist some positive integer n with the property that

$$x + y\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n. \tag{192}$$

Proof. Let $(x, y) \in \mathbb{N}^2$ be an arbitrary solution to equation (191). Since $x_1 + \sqrt{d}y_1 > 1$ is smaller than $x + \sqrt{d}y$ (due to the minimality of y_1 and implicitly of x_1 among solutions to equation (191)), then there exists a unique positive integer n such that

$$\left(x_1 + \sqrt{d}y_1\right)^n \le x + \sqrt{d}y < \left(x_1 + \sqrt{d}y_1\right)^{n+1}. \tag{193}$$

We let x_0 and y_0 be integers such that:

$$x_0 + \sqrt{d}y_0 := \left(x + \sqrt{d}y\right) \cdot \left(x_1 - \sqrt{d}y_1\right)^n. \tag{194}$$

First, we note that indeed when expanding the right-hand side of identity (194), we get an expression of the form $A + \sqrt{d}B$ for some integers A and B; hence, x_0 and y_0 are well-defined by (194).

Secondly, we recall the identity

$$(A \pm \sqrt{d}B) \cdot (C \pm \sqrt{d}D) = (AC + dBD) \pm \sqrt{d} \cdot (AD + BC), \tag{195}$$

which means that if $A^2 - dB^2 = 1$ and $C^2 - dD^2 = 1$, then also

$$(AC + dBD)^2 - d \cdot (AD + BC)^2 = 1. \tag{196}$$

So, using that $x^2 - dy^2 = 1$ along with the fact that

$$x_1^2 - d(-y_1)^2 = x_1^2 - dy_1^2 = 1,$$

then using repeatedly (precisely n times) the identities from (195) and (196), we conclude that

$$x_0^2 - dy_0^2 = 1. \tag{197}$$

Now, using the definition for x_0 and y_0 in (194) along with the inequalities from (193) and the fact that

$$\left(x_1 + \sqrt{d}y_1\right)^n \cdot \left(x_1 - \sqrt{d}y_1\right)^n = \left(x_1^2 - dy_1^2\right)^n = 1,$$

we get that

$$1 \le x_0 + \sqrt{d}y_0 < x_1 + \sqrt{d}y_1. \tag{198}$$

Clearly, the right-hand side of the inequality (198) yields that not both x_0 and y_0 can be positive integers since otherwise we would contradict the minimality of y_1 (and implicitly of x_1).

Claim 24.7. *With the above notation, we have that $y_0 \ge 0$.*

Proof of Claim 24.7. We argue by contradiction and therefore assume that $y_0 < 0$ and then derive a contradiction.

Now, if also x_0 were negative, then clearly the left-hand side of inequality (198) would be contradicted; so, we must have then $x_0 \geq 0$.

On the other hand, $x_0^2 - dy_0^2 = 1$ (according to (197)), which means that actually $x_0 \geq 1$ and furthermore, using our assumption that $y_0 < 0$, we then get

$$x_0 + \sqrt{d}y_0 = \frac{1}{x_0 - \sqrt{d}y_0} < \frac{1}{x_0} \leq 1,$$

which contradicts the left-hand side in the inequality (198). So, indeed we must have that $y_0 \geq 0$, as claimed. □

Now, using (197), we get that

$$|x_0| > \sqrt{d} \cdot y_0 \tag{199}$$

(note that $y_0 \geq 0$ by Claim 24.7). So, we cannot have that $x_0 < 0$ because then (199) would force $x_0 + \sqrt{d}y_0 < 0$, contradicting the left-hand side of inequality (198). Thus $x_0 > 0$ (note that x_0 cannot be 0 due to inequality (199)). Now, since we have that $x_0 \in \mathbb{N}$ and $y_0 \geq 0$, *but* $(x_0, y_0) \notin \mathbb{N}^2$ (because then we contradict the minimality of y_1, as discussed), then the only possibility is that $y_0 = 0$ and because $x_0 > 0$ satisfies (190), we must have that $x_0 = 1$. So,

$$x + \sqrt{d}y = \left(x_1 + \sqrt{d}y_1\right)^n,$$

as desired in the conclusion of Proposition 24.6. □