

Math 215: Theorem Packet

Hunter Hawkins-Stark
Vandal Number V00655052

August 7, 2020

1 Proof of The Division Algorithm

Claim: Let a, b be integers with b not equal to zero. Then, there exists a unique pair of integers q and r , such that $a = b \cdot q + r$ and $0 \leq r < |b|$

Proof: Let a and b be integers with b not equal to zero. If $b = 1$, then $q = a$, so we will assume that $b > 1$. Then there exists a set S of the form $a - k \cdot b$, where k is an integer, and the set S contains all natural numbers that fit the form.

We must now show that S is non-empty, because if S is non-empty the well ordering principle will give us the least element of S . This least element will be r .

Case 1: $a \geq 0$, so we will set $k = 0$, plugging into our formula we get $a - 0 \cdot b$. The solution is then simply just a , which means that $a \geq 0$ of S , thus the set S is non-empty.

Case 2: $a < 0$, so we will set $k = a$. Plugging into our formula we get $a - kb$, with k being equal to a we once again substitute to get $a - ab$. Factoring out an a gives us the form $a(1 - b)$, and due to $a < 0$ and $b > 1$, $a(1 - b)$ must be greater than 0 of S . Thus the set S is non-empty.

With both cases of a either being greater than 0, and being less than zero resulting in a non-empty empty set S , S must have a least element r which is equal to $a - qb$ for some integer q . Thus $a = q \cdot b + r$ and $r \geq 0$. Now we need to show that $r < b$, and that q and r are unique.

Show $r < b$: Suppose $r \geq b$, then $r = b + z$, where z is an integer that fits the form of $0 \leq z < r$. Using our original equation $a = q \cdot b + r$ and the fact that $r = b + z$ we perform a substitution for r in the original equation resulting in $a = q \cdot b + b + z$. Simplifying we arrive at the result $z = a - (q + 1) \cdot b$ which is also an element of our set S , and is smaller than r . Using this we arrive at a contradiction where r is not the least element of S , thus $r < b$.

Show q and r are unique: Let there exist integers x and y that satisfy $a < xb + y$ and $0 \leq y < b$. Using the assumption of $y \geq r$ we get $0 \leq r - y < b$. With $xb + y$ being equal to $qb + r$ we get $r - y = b(x - q)$. With us knowing $0 \leq r - y < b$, we then know b divides $r - y$. This $y = r$ and $x = q$ and thus they are unique.

QED

2 Proof of the Euclidean Algorithm

Claim: Suppose $a, b \in \mathbb{N}$. If we repeatedly perform the division algorithm:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\dots \\ &\dots \\ r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1} \\ r_{n-2} &= r_{n-1}q_n + 0 \\ r_{n-1} &= \gcd(a, b) \end{aligned}$$

Prove that $r_{n-1} = \gcd(a, b)$

Proof: Let $a, b \in \mathbb{N}$ and $d \in \mathbb{Z}$. First we notice that the sequence $\{r_1, r_2, \dots\} \subseteq \mathbb{N}$ and is decreasing. Thus it truncates at a certain point, and this point is at r_{n-1} . Next we want to show that $r_{n-1} \mid a$ and $r_{n-1} \mid b$. Using the equation $r_{n-2} = r_{n-1}q_n + 0$ we can see $r_{n-1} \mid r_{n-2}$ we can also see that $r_{n-1} \mid r_{n-3}$ which if we continue on we find that $r_{n-1} \mid a$ and $r_{n-1} \mid b$. Now that we know the sequence ends at a point (ie r_{n-1} exists) and that point is a divisor of a and b we need to prove its the greatest common divisor of a and b . Let $d \mid a$ and $d \mid b$. This means that $d \mid a - bq_1$ which when rearranging the equation $a = bq_1 + r_1$ means that $d \mid r_1$ (d divides the first non zero remainder). Also $d \mid b - r_1q_1$ which once again after rearranging means $d \mid r_2$ (d divides the second non zero remainder). Following this trend we arrive at $d \mid r_{n-1}$ thus, $r_{n-1} = \gcd(a, b)$.

QED

3 Proof of the Fundamental Theorem of Arithmetic

Claim: Let $n \in \mathbb{Z}$ excluding $\{0, +1, -1\}$. Then \exists prime numbers p_1, \dots, p_k such that $n = \prod_{i=1}^k p_i$

Proof: This proof will be done by induction, and will use Lemma 1 that states if an integer is greater than 1, then it can be written as a product of primes uniquely apart from the ordering of the primes. Let $n \in \mathbb{Z}$ excluding $\{0, +1, -1\}$

Base case: Let $n = 2$. Then n can be written as a product of a single prime number which is 2.

Inductive Step: First we will assume that every integer between 2 and K can be written as a product of one or more primes. Now for induction we need to show that $k+1$ can be written as a product of primes.

Case 1: $K + 1$ is prime. Then it is the product of one prime, which is itself.

Case 2: $K + 1$ is composite. Then $\exists a, b$ which are $\in \{a, b \in \mathbb{Z} \mid a \geq 2, b \geq 2\}$. By induction a can be written as a product of primes p_1, \dots, p_r and b can be written as a product of primes q_1, \dots, q_s such that $p_1 \leq \dots \leq p_r$ and $q_1 \leq \dots \leq q_s$. With $k + 1$ being composite we know it can be written as a product of primes according to lemma 1. In our specific case $k + 1$ can be written as $a * b$, which is equivalent to $p_1, \dots, p_r * q_1, \dots, q_s$ which is a product of primes. Thus $k + 1$ can be represented by a product of primes when composite.

Now that we have shown there exists a solution, we want to show there is a unique prime factorization for n . We will also do this by induction.

Let $P(k)$ be the statement that if $p_1, \dots, p_r = q_1, \dots, q_s$ where $p_1 \leq \dots \leq p_r$ and $q_1 \leq \dots \leq q_s$ then $r = s$ and $p_i = q_i$ for all $i \in \mathbb{N}$ with $1 \leq i \leq k$

Base case: Show $P(1)$ is a true statement. First let $p_1 = q_1, \dots, q_s$ where p_1 is prime along with q_1, \dots, q_s . With p_1 being prime, we have that $s = 1$ and thus $p_1 = q_1$.

Inductive Step: Now we will assume $P(k)$ is true in order to show $P(k+1)$ is true. For $P(k+1)$ we will assume that $p_1, \dots, p_{k+1} = q_1, \dots, q_t$ for the prime numbers p_1, \dots, p_{k+1} and q_1, \dots, q_t that follow the conditions of $p_1 \leq \dots \leq p_r$ and $q_1 \leq \dots \leq q_t$. Due to $K \geq 1$ we know p_1, \dots, p_{k+1} is not prime, and thus $t \geq 2$. Let p be the largest prime such that $p \mid p_1, \dots, p_{k+1}$, which then follows that $p \mid p_i$ where i is an integer and $1 \leq i \leq K + 1$. Since p_i is prime, we know $p = p_i$ which then results in $p = p_i \leq p_{k+1}$. Also in the choice of p , we have $p \geq p_{k+1}$ which follows that $p = p_{k+1}$. By the same logic we know that $p = q_t$ and thus $p_{k+1} = q_t$. Then $p_1, \dots, p_k = q_1, \dots, q_{t-1}$. Via the induction hypothesis, we have that $k = t - 1$ and that $p_i = q_i$ for all i within $1 \leq i \leq k + 1$.

Thus we have shown that if $P(k)$ has a solution and that it is unique, then $P(k+1)$ also has a unique solution. By the principle of mathematical induction, $P(K)$ for all k in the natural numbers must be true.

QED

4 Euclids proof of Infinitely Many Prime Numbers

Claim: Prove there is infinitely many prime numbers

Proof: This proof will be by contradiction. Let $p_1, p_2, \dots, p_n \in \mathbb{Z}$ and suppose for contradiction that there are only a finite amount of primes. We will write them as p_1, p_2, \dots, p_n . Then let $q = p_1 p_2 \dots p_n + 1$. Then q cannot be prime as $q \notin \{p_1, \dots, p_n\}$, however q will have a prime factor, which we will call p_k where $p_k \in \{p_1, \dots, p_n\}$. So p_k is a factor of q , p_k is also a factor of $p_1 p_2 \dots p_n$, and thus p_k is a factor of $q - p_1 p_2 \dots p_n$. However since $\frac{q - p_1 p_2 \dots p_n}{p_k} = \frac{1}{p_k}$, and $\frac{q - p_1 p_2 \dots p_n}{p_k} \in \mathbb{Z}$ but $\frac{1}{p_k} \notin \mathbb{Z}$ we have arrived at a contradiction.

Thus there must be infinitely many prime numbers.

QED

5 Modular Arithmetic is Well Defined Over Addition and Multiplication

Addition Claim: If $a \equiv b \pmod n$ and $c \equiv d \pmod n$ then $a + c \equiv b + d \pmod n$

Addition Proof: Let $a, b, c, d, n \in \mathbb{Z}$. Then by congruence $\exists s, t \in \mathbb{Z}$ such that $a - b = sn$ and $c - d = tn$. Adding these two statements together we get $(a - b) + (c - d) = sn + tn$. Adding $(b + d)$ to each side we get $a + c = b + d + sn + tn$. Factoring n out of the right side we get $a + c = b + d + n(s + t)$. Then by definition of congruence modulo n , $a + c \equiv b + d \pmod n$. Thus, addition is well defined modulo n .

QED

Multiplication claim: If $a \equiv b \pmod n$ and $c \equiv d \pmod n$ then $a * c \equiv b * d \pmod n$

Multiplication Proof: Let $a, b, c, d, n \in \mathbb{Z}$. Then by definition of congruence we know $a = nz + b$ and that $c = ny + d$ for $z, y \in \mathbb{Z}$. Multiplying these two statements together we get $ac = nzn y + nzd + nyb + bd$. Then after simplifying and rearranging we get $ac - bd = n(zny + zd + yb)$ which shows $n \mid ac - bd$ and thus by definition of congruence modulo n , $ac \equiv bd \pmod n$. This proves that multiplication is well defined modulo n .

QED

6 Proof of the Chinese Remainder Theorem

Claim: Let $r \in \mathbb{N}$, $n_1, \dots, n_r \in \mathbb{N}$, and $a_1, \dots, a_r \in \mathbb{Z}$. Let the $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of congruences

$$x \equiv a_i \pmod{n_i} \text{ where } i \in \{1, \dots, r\}$$

has a unique solution modulo $\prod_{i=1}^r n_i$.

Proof: This proof will be done by using induction on r . Let $x \in \mathbb{Z}$, $r \in \mathbb{N}$, and $a_1, \dots, a_r \in \mathbb{Z}$. Let $Q(r)$ be the fact that $x \equiv a_i \pmod{n_i}$ for $i \in 1, \dots, r$ has a solution modulo $\prod_{i=1}^r n_i$ whenever the $\gcd(n_i, n_j) = 1$ for $i \neq j$.

Base Case: Let the $\gcd(n_i, n_j) = 1$ for all $i \neq j$. With the system of congruences $x \equiv a_i \pmod{n_i}$ for $i \in 1, 2$, a solution can only be found if and only if $\gcd(n_1, n_2) \mid (a_1 - a_2)$. Also that solution modulo $n_1 n_2$ is unique only when $\gcd(n_1, n_2) = 1$. Thus when $r = 2$ the statement holds, which in return proves our base case.

Induction Step: Suppose that $x \equiv a_i \pmod{n_i}$ where $i \in \{1, \dots, r\}$ has a solution modulo $\prod_{i=1}^r n_i$. Now using PMI, we must consider the system of congruences with $x \equiv a_i \pmod{n_i}$ where $i \in \{1, \dots, r+1\}$. By the inductive hypothesis there is a solution Y in which $Y \equiv a_i \pmod{n_i}$ for all $i \in \{1, \dots, r+1\}$. Using this fact and the fact that $x \equiv a_{i+1} \pmod{n_{i+1}}$ we know the two systems of congruences have a unique solution Z . Which means $Z \equiv a_i \pmod{n_i}$ for all $i \in \{1, \dots, r+1\}$ and Z is a unique solution determined using modulo $\prod_{i=1}^{r+1} n_i$.

Thus by the principle of mathematical induction Z has a unique solution. Every other solution to the system is congruent to Z modulo $\prod_{i=1}^r n_i$.

QED

7 Proof of Euler's Theorem

Claim: Let m and $a \in \mathbb{Z}$ and suppose that $m \geq 1$ and $\gcd(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof: From proving lemma 2 we know that $r_1, r_2, \dots, r_{\phi(m)} \equiv (ar_1)(ar_2), \dots, (ar_{\phi(m)})$ which also means $r_1, r_2, \dots, r_{\phi(m)}$ is equivalent to $a^{\phi(m)}(r_1 r_2 \dots r_{\phi(m)}) \pmod{m}$. Due to each of $r_1, r_2, \dots, r_{\phi(m)}$ being relatively prime to m , it follows that their product is as well. Hence that factor can be canceled in the last congruence and we get $1 \equiv a^{\phi(m)} \pmod{m}$

QED

8 Proof of Fermats Little Theorem (A Special Case of Eulers Theorem)

Claim: Let n be a prime and $a \in \mathbb{Z}$. Assume $n \nmid a$, then $a^{n-1} \equiv 1 \pmod{n}$

Proof: Using Eulers theorem (proven above) we have the formula $a^{\phi(n)} \equiv 1 \pmod{n}$. In our case we are dealing with a prime number, which gives us $\phi(n) = n - 1$. Substituting this into our equation we get $a^{n-1} \equiv 1 \pmod{n}$. Which then proves Fermats little theorem.

QED

9 There are $\phi(p-1)$ primitive roots mod p

Claim: Every prime p has $\phi(p-1)$ primitive roots.

Proof: Lemma 6 states that each integer $1, 2, \dots, p-1$ has an order that is a divisor of $p-1$. For each divisor r of $p-1$, let $\psi(r)$ represent the number of integers in $1, 2, \dots, p-1$ that have order r. From Lemma 7 we know that $\sum_{r|p-1} \psi(r) = \sum_{r|p-1} \phi(r)$. It will follow from this equation that if we can show $\psi(r) \leq \phi(r)$ we can conclude that $\psi(r) = \phi(r)$ for each r. The number of primitive roots of p will be $\psi(p-1) = \phi(p-1)$. From here we will choose an r.

Case 1: if $\psi(r) = 0$ then $\psi(r) < \phi(r)$ and we have proved what we needed to prove.

Case 2: If $\psi(r) \neq 0$, then there is an integer with order r, which we will call a. The congruence $x^r \equiv 1 \pmod p$ has exactly r solutions according to lemma 4. Also, $x^r \equiv 1 \pmod p$ is satisfied by the r integers a, a^2, a^3, \dots, a^r , where they all give solutions as no two of these have the same least residue mod p. From lemma 5, the numbers in a, a^2, a^3, \dots, a^r have order r are those powers a^k with the $\gcd(k, r) = 1$. However, there are $\phi(r)$ such numbers k. Hence $\psi(r) = \phi(r)$ in this case.

Thus, we know every prime number p has $\phi(p-1)$ primitive roots.

QED

10 There are 2 solutions or no solutions to the congruence $x^2 \equiv a \pmod p$ with $p \nmid a$

Claim: There are either 2 solutions or no solutions to the congruence $x^2 \equiv a \pmod p$ for a prime number p and an integer a with $p \nmid a$. Further the congruence has solutions iff $a^{(p-1)/2} \equiv 1 \pmod p$

proof: Let p be an odd prime number, let g be a primitive root, and let $x, l \in \mathbb{Z}$. First we should move a to the other side of the congruence which gives us $x^2 - a \equiv 0 \pmod p$. From here we know by definition of congruence that $p \mid x^2 - a$, which is the same as $p \mid (x - a) * (x + a)$. Then due to p being prime we know that $p \mid (x - a)$ or $p \mid (x + a)$. Thus by definition of congruence x must have two or no solutions as $x \equiv a \pmod p$ or $x \equiv -a \pmod p$. a is a square modulus p if and only if $a \equiv g^{2l}$. Thus $a^{(p-1)/2} \equiv (g^{2l})^{(p-1)/2} \equiv (g^{p-1})^l \equiv 1$ If a is a square and $a^{(p-1)/2} \equiv (g^{2l+1})^{(p-1)/2} \equiv (g^{p-1})^l * g^{(p-1)/2} \equiv -1$

Thus there are either 2 solutions or no solutions to the congruence $x^2 \equiv a \pmod p$ for a prime number p and an integer a with $p \nmid a$, and further the congruence has solutions iff $a^{(p-1)/2} \equiv 1 \pmod p$.

QED

11 Lemmas

Lemma 1: Let n be an integer. Every $n > 1$ is equal to a product of prime numbers (potentially just one prime number).

Proof: This proof is by contradiction. Assume that there is at least one integer greater than 1, we will call it M , that is not equal to the product of primes. Since M is not equal to the product of prime numbers, then M must be composite. Then $\exists a, b \in \mathbb{Z}$ such that $m = ab$, $1 < a < m$, and $1 < b < m$. Although, m was the smallest integer greater than one that was not equivalent to a product of primes, and thus a and b must be equivalent to a product of primes. Hence $m = a * b$ has to be equivalent to a product of primes, and thus leads us to a contradiction.

Thus we know every integer that is greater than 1 is equivalent to the product of prime numbers (it may potentially be one).

QED

Lemma 2: If the $\gcd(a, m) = 1$ and $r_1, r_2, \dots, r_{\phi(m)}$ are the positive integers less than m and relatively prime to m , then the least residues mod m of $ar_1, ar_2, \dots, ar_{\phi(m)}$ are a permutation of $r_1, r_2, \dots, r_{\phi(m)}$.

Proof: Do to their being exactly $\phi(m)$ numbers in the set, to prove that their least residues are a permutation of $\phi(m)$ numbers $r_1, r_2, \dots, r_{\phi(m)}$. We have to show that they are all relatively prime to m and show that they are all different.

Prove all numbers are relatively prime to m : Let p be a prime number that is a common divisor of ar_i and m for some i where $1 \leq i \leq \phi(m)$. With p being prime, we know either $p \mid a$ or $p \mid r_i$. This tells us that either p is a common divisor of a and m or p is a common divisor of m and r_i . However, with the $\gcd(r_i, m) = 1$ and the $\gcd(a, m) = 1$ this means the possibility of p being a common divisor in any case is a contradiction. Thus the $\gcd(ar_i, m) = 1$ for each i $1 \leq i \leq \phi(m)$.

Prove all are different: Let i and $j \in \mathbb{Z}$ where $1 \leq i \leq \phi(m)$ and $1 \leq j \leq \phi(m)$ such that $ar_i \equiv ar_j \pmod{m}$. Due to the $\gcd(a, m)$ being one, we can cancel a from both sides in order to get $r_i \equiv r_j \pmod{m}$. With $r_i = r_j$ we know that if $r_i \neq r_j$ then $ar_i \not\equiv ar_j \pmod{m}$ and thus all the numbers are different.

Thus we know that the least residues mod m of $ar_1, ar_2, \dots, ar_{\phi(m)}$ are a permutation of $r_1, r_2, \dots, r_{\phi(m)}$.

QED

Lemma 3: If f is a polynomial of degree n , then $f(x) \equiv 0 \pmod{p}$ has at most n solutions

Proof: This proof will be on induction on the degree n . Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ have degree n so that $a_n \not\equiv 0 \pmod{p}$.

Base Case: For $n = 1$ $a_1 x + a_0 \equiv 0 \pmod{p}$ has only one solution since the $\gcd(a_1, p) = 1$.

Inductive Hypothesis: Let the lemma be true for polynomials of degree $n-1$, and let f have degree n . Then Either $f(x) \equiv 0 \pmod{p}$ has no solutions or it has atleast one solution.

Case 1: $f(x) \equiv 0 \pmod{p}$ has no solutions, thus the lemma is true.

Case 2: Let y be a solution such that $f(y) \equiv 0 \pmod{p}$ where y is a least residue mod p . Then due to $x - y$ being a factor of $x^z - y^z$ for $z = 0, 1, \dots, n$ we have $f(x) \equiv f(x) - f(y)$. After substituting and simplifying we end up with $f(x) \equiv a_n(x^n - y^n) + a_{n-1}(x^{n-1} - y^{n-1}) + \dots + a_1(x - y)$. Finally we get $f(x) \equiv (x - y)h(x) \pmod{p}$ where h is a polynomial of degree $n-1$. If we let w be a solution of $f(x) \equiv 0 \pmod{p}$ we get $f(w) \equiv (w - y)h(w) \equiv 0 \pmod{p}$. Due to p being prime we know $w \equiv y \pmod{p}$ or $h(w) \equiv 0 \pmod{p}$. From the induction assumption, the second congruence has at most $n-1$ solutions. Due to the first congruence having just one solution, we have proved $f(x) \equiv 0 \pmod{p}$ has at most n solutions.

Thus by PMI, If f is a polynomial of degree n , then $f(x) \equiv 0 \pmod{p}$ has at most n solutions.

QED

Lemma 4: If $d \mid p - 1$, then $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

Proof: Using Fermats theorem, $x^{p-1} \equiv 1 \pmod{p}$ has exactly $p-1$ solutions, specifically $1, 2, \dots, p-1$. Further, $x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + x^{p-1-2d} + \dots + 1)$, then $x^{p-1} - 1 = (x^d - 1)g(x)$. From our third lemma we know that $g(x) \equiv 0 \pmod{p}$ has at most $p - 1 - d$ solutions. Hence $x^d \equiv 1 \pmod{p}$ has atleast d solutions. If we apply lemma 3 again we see that $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

Thus, If $d \mid p - 1$, then $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

QED

Lemma 5: Suppose that a has order $t \pmod{m}$. Then a^k has order $t \pmod{m}$ if and only if the $\gcd(k, t) = 1$.

Proof: Suppose that the $\gcd(k, t) = 1$ and denote the order of a^k by s . We have that $1 \equiv (a^t)^k \equiv (a^k)^t \pmod{m}$, so we know $s \mid t$ as s is the order of a^k . Then we have $(a^k)^s \equiv a^{ks} \equiv 1 \pmod{m}$. We know $t \mid ks$ due to the $\gcd(k, t) = 1$ it follows that $t \mid s$. This fact, along with $s \mid t$ implies that $s = t$. To prove the converse, let a and a^k have order t and that the $\gcd(k, t) = r$. Then $1 \equiv a^t \equiv (a^t)^{t/r} \pmod{m}$. Due to the order of a^k we know that $t \mid r$ is a multiple of t which implies that $r = 1$.

Thus, If a has order $t \pmod{m}$, then a^k has order $t \pmod{m}$ if and only if the $\gcd(k, t) = 1$.

QED

Lemma 6: If $\gcd(a, m) = 1$ and a has order $t \bmod m$, then $t \mid \phi(m)$.

Proof: Using Eulers extension of Fermats Theorem we know that $a^{\phi(m)} \equiv 1 \bmod m$. Which allows us to conclude $\phi(m)$ is a multiple of t . Thus we know that $t \mid \phi(m)$

Thus, If $\gcd(a, m) = 1$ and a has order $t \bmod m$, then $t \mid \phi(m)$.

QED

Lemma 7: If $n \geq 1$ then, $\sum_{d \mid n} \phi(d) = n$

Proof: We have m in C_d if and only if the $\gcd(m, n) = d$. However, the $\gcd(m, n) = d$ if and only if $(m/d, n/d) = 1$. This means an integer m is in class C_d if and only if m/d is relatively prime to n/d . The number of positive integers $\leq n/d$ and relatively prime to n/d is $\phi(n/d)$ by definition. This the number of elements in class C_d is $\phi(n/d)$.

Thus, If $n \geq 1$ then, $\sum_{d \mid n} \phi(d) = n$

QED