Math 215: Theorem Packet

Hunter Hawkins-Stark
Vandal Number V00655052

July 29, 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 then 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 Extended Euclidean Algorithm

Claim: If d divides a, d dives b, and $d = ax + by$ for some integers x and y, the d = gcd(a,b).

Proof: Let there exist integers a, b,x,y, and d, such that d divides a, d divides b, and d = ax+by. We want to show that d = gcd(a,b) With d dividing both a and b, d cannot exceed the greatest common divisor which means that $d \leq gcd(a, b)$. Also, since the gcd(a,b) is a common factor of a and b, it must also divide $ax + by$. Using this we get $gcd(a, b) \leq d$. After finding the facts that $d \leq gcd(a, b)$ and $gcd(a, b) \leq d$ we can conclude that $d = gcd(a, b)$.

QED

3 Proof of the Fundamental Theorem of Arithmetic

Claim: If a is an integer larger than 1, then a can be written as a product of primes. Furthermore, this factorization is unique except for the order of the factors.

Proof: This proof will be divided up into two parts, each of which will use the well-ordering principle for the set of natural numbers. First we will prove that every a >1 can be written as a product of prime factors. Then we will prove that this factorization is unique except for reordering of the factors. Let there exist an integer z, which is greater than 1, that cannot be written as a product of primes. Using the well ordering principle there is a smallest z that fits the criteria, thus z is not prime so z = b*cdot*c where 1 < b and c < a for a and b being integers. So b and c can be written as a product of prime factors due to z being the smallest integer than cannot be, but since z = b · c this makes a contradiction as the equation makes z a product of prime factors. In order to prove uniqueness let there exist an integer z > 1 that has two different prime factorizations, say $z = p_1...p_k$ and $z = q_1...q_t$ where $p_1...p_k$ and $q_1...q_t$ are all primes. Thus $p_1|q_1...q_t$, and since p_1 is prime, $p_1, |q_j$ for some integer k. Since q_j is prime and $p_1 > 1$, this means $p_1 = q_1$. Using that fact we can cancel p_1 from both sides of the equation to get $p_2...p_k = q_2...q_t$. With the assumption being that a is the smallest positive integer with a non-unique prime factorization, $p_2...p_k < a$, $p_2...p_k = q_2...q_t, k = t$ and $p_1 = q_1$ we arrive at a contradiction to the assumption that these were two unique factorizations as they are equivalent.

QED

4 Proof of the Chinese Remainder Theorem

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

$$x \equiv a_i \ mod \ n_i \text{ where } i \in \{1, ...r\}$$

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

Proof: This proof will be done by using induction on r. Let x $\in \mathbb{Z}, r \in \mathbb{N}$, and $a_1, ..., a_r \in \mathbb{Z}$. Let Q(r) be the fact that $x \equiv a_i mod n_i$ for $i \in 1, ..., r$ 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 $x \equiv a_i mod n_i$ 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 $x \equiv a_i mod n_i$ where $i \in$ {1,...r} has a solution module $\prod_{i=1}^{r} n_i$.Now using PMI, we must consider the system of congruences with $x \equiv a_i mod n_i$ where $i \in \{1, ...r + 1\}$ By the inductive hypothesis there is a solution Y in which $Y \equiv a_i \ mod \ n_i$ for all $i \in \{1, ...r + 1\}$. Using this fact and the fact that $x \equiv a_{i+1} \ mod \ n_{r+1}$ we know the two systems of congruences have a unique solution Z. Which means $Z \equiv a_i \ mod \ n_i$ for all $i \in \{1, ...r + 1\}$ 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

5 Proof of Euler's Theorem

Claim: Let n $\geq$ be an integer and a $\in \mathbb{Z}$ with $gcd(a, n) = 1$. Then we wish to prove three core points to get a conclusive proof. First we wish to prove $\{b\ mod\ n \mid b \in \mathbb{Z}, gcd(b, n) = 1\} = \{ab\ mod\ n \mid b \in \mathbb{Z}, gcd(b, n) = 1\}$. Secondly is to prove if B = $\{b \mid 1 \leq b \leq n - 1\ with\ gcd(b, n) = 1\}$ then

$$\prod_{b \in B} ab \equiv \prod_{b \in B} b\ mod\ n$$

After proving these two we will be able to show and prove that $a^{\phi(n)} \equiv 1\ mod\ n$

Proof: For the first section of this proof we want to show equivalence between $\{b\ mod\ n \mid b \in \mathbb{Z}, gcd(b, n) = 1\}$ and $\{ab\ mod\ n \mid b \in \mathbb{Z}, gcd(b, n) = 1\}$. Let X= $\{b\ mod\ n \mid b \in \mathbb{Z}, gcd(b, n) = 1\}$ and Y = $\{ab\ mod\ n \mid b \in \mathbb{Z}, gcd(b, n) = 1\}$. Then we will number of elements of the sets with the ϕ function, which then has the elements of X as $b_1, ..., b_{\phi(n)}$ and the elements of Y being $ab_1, ..., ab_{\phi(n)}$. We must now show that the $gcd(ab_i, n) = gcd(b_i, n) = 1$ and that $ab_i \not\equiv ab_j\ mod\ n$ for all $i \neq j \in \{1, ..., \phi(n)\}$. For the second condition we will suppose that $ab_i \equiv ab_j\ mod\ n$ then, a is invertible modulo n, $b_i \equiv b_j\ mod\ n$ and that $b_i = b_j$. Further $ab_i \not\equiv ab_j\ mod\ n$ whenever $b_i \neq b_j$. In order to show the $gcd(ab_i, n) = gcd(b_i, n) = 1$, we will assume that $p \mid a$ or $p \mid b_i$ which results in a contradiction as $gcd(ab_i, n) = gcd(b_i, n) = 1$ means we have p = 1, and this is a contradiction. In conclusion we know that all elements of Y are distinct modulo n and that the $gcd(ab_i, n) = 1$ for all i, which means X = Y. This proves ($\{b\ mod\ n \mid b \in \mathbb{Z}, gcd(b, n) = 1\} = \{ab\ mod\ n \mid b \in \mathbb{Z}, gcd(b, n) = 1\}$).

Using what we just proved $ab_1, ..., ab_{\phi(n)} \equiv b_1, ..., b_{\phi(n)} mod\ n$, and combining terms we can get $a^{\phi(n)} b_1, ..., b_{\phi(n)} \equiv b_1, ..., b_{\phi(n)} mod\ n$. With all $b \in B$ being invertible mod n we can conclude that $a^{\phi(n)} \equiv 1\ mod\ n$, which thus proves Eulers theorem.

QED

6 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 $a^{n-1} \equiv 1 \ (mod\ n)$

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

QED