Math 335 Assignment 12

Arnold Jiadong Yu

May 3, 2018

(1) Let $n \geq 2$ be a natural number and $a_1, ..., a_n$ be integers, not all zero. Show that there are integers $x_1, .., x_n$ such that

$$(gcd)(a_1, ..., a_n) = x_1 a_1 + ... + x_n a_n$$

proof: Let J be the set of all the linear combinations of $a_1, ..., a_n$ and $J \subseteq \mathbb{Z}$. J is closed with respect to addition and negatives and absorbs products since

$$(x_1 a_1 + ... + x_n a_n) + (y_1 a_1 + ... + y_n a_n) = (x_1 + y_1)a_1 + ... + (x_n + y_n)a_n$$

$$-(x_1 a_1 + ... + x_n a_n) = (-x_1)a_x + ... + (-x_n)a_n$$

$$z(x_1 a_1 + ... + x_n a_n) = (zx_1)a_1 + ... + (zx_n)a_n$$

Therefore, J is an ideal of $\mathbb{Z}$. Since every ideal of $\mathbb{Z}$ is principle, then J is a principle ideal of $\mathbb{Z}$. Hence $\exists t \in \mathbb{Z}$ such that $J = (t)$. t is in J, then t is a linear combination of all elements in J. Therefore

$$t = x_1 a_1 + ... + x_n a_n$$

That is t is a common divisor of $a_1, ..., a_n$. If there is another common divisor u, then $a_1 = uc_1, ..., a_n = uc_n$, this means $u|t$. Therefore, t must be $(gcd)(a_1, ..., a_n)$. Hence there are integers $x_1, .., x_n$ such that $(gcd)(a_1, ..., a_n) = x_1 a_1 + ... + x_n a_n$.

(2) Let $p \geq 2$ be a prime number. Show that, for every $k = 1, ..., p-1$, the binomial coefficient $\binom{p}{k}$ is divisible by p.

proof: By how binomial coefficient was derived. $\binom{p}{k} = r \in \mathbb{N}$. Moreover, $\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)...(p-k+1)}{k!}$. Since $k < p$ and p is prime, then k will not divide p for all $0 < k < p$. Therefore, the prime number p will not be reduced. Hence $p|\binom{p}{k}$.

(3) Let $p \geq 2$ be a prime number and a be an arbitrary integer. Show that p divides $a^p - a$.

proof: Prove by induction. W.L.O.G. Assume $a \geq 0$, when $a = 0$ or 1, $a^p - a = 0$ is divisible by any $p \geq 2$. Assume p divides $a^p - a$, then

$$(a+1)^p - (a+1) = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-1} + ... + \binom{p}{p-1}a + 1 - a - 1$$

$$= a^p - a + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-1} + ... + \binom{p}{p-1}a$$

Since $a^p - a$ is divisible by p, and for any $p \geq 2$, the binomial coefficient is divisible by p. Therefore, the right side of the equation is divisible by p. Hence $(a+1)^p - (a+1)$ is divisible by p. As a result, let $p \geq 2$ be a prime number and a be an arbitrary integer, then p divide $a^p - a$.

(4) Let $n \geq 2$ be an integer, such that n divides $(n-1)! + 1$. Show that n is prime.

proof: Prove by contradiction. Assume n is not prime, then n has its unique factorization. Let $n = \prod_{i=1}^{N} p_i$, then $2 \leq p_1 \leq n - 1$ for $1 \leq i \leq N$. W.L.O.G, pick p_1. n divides $(n-1)! + 1$ means p_1 divides $(n-1)! + 1$ and

$$(n-1)! \equiv -1(\bmod p_1)$$

But $n = \prod_{i=1}^{N} p_i$ and $2 \leq p_1 \leq n - 1$ for $1 \leq i \leq N$, then

$$(n-1)! \equiv 0(\bmod p_1)$$

There is an contradiction. Hence n must be prime.

(5) Let $p \geq 3$ be a prime number. Show that either $p - 1$ or $p + 1$ is divisible by 6.

proof: Since p is a prime number greater or equal to 3, then p is odd prime. Therefore, both $p-1$ and $p+1$ is even. That is $2|(p-1)$ and $2|(p+1)$. Moreover, 3 must divide one of the three number $p-1, p, p+1$. p is prime, then 3 must divide one of the two $p-1, p+1$. Since both of them are divisible by 2. Hence either $p-1$ or $p+1$ is divisible by $2 \cdot 3 = 6$.

(6) Let $n \geq 2$ be a natural number. An *elementary transformation* of n-tuple of integers $\mathbf{b}$ by changing a component b_i to $b_i + cb_j$ for some $j \neq i$ and $c \in \mathbb{Z}$. Let $a_1, ..., a_n$ be integers, such that $\gcd(a_1, ..., a_n) = 1$. Show that there is a sequence of elementary transformation, transforming the n-tuple $\mathbf{a} = (a_1, ..., a_n)$ to the n-tuple $(1, 0, ..., 0)$.

proof: $\gcd(a_1, ..., a_n) = 1$. It is the same as

$$\gcd(a_1, a_2, ..., a_n) = \gcd(a_1, \gcd(a_2, \gcd(a_3, ..., \gcd(a_{n-1}, a_n)))) = 1$$

By Eucildean algorithm, we can transform (a_{n-1}, a_n) to $(\gcd(a_{n-1}, a_n), 0)$ as following. W.L.O.G. Assume $a_n \geq a_{n-1}$, then by division algorithm,

$$a_n = a_{n-1}q_1 + r_1, \text{ for some } q_1, r_1 \in \mathbb{Z}$$

$$a_{n-1} = r_1 q_2 + r_2, \text{ for some } q_2, r_2 \in \mathbb{Z}$$

$$r_1 = r_2 q_3 + r_3, \text{ for some } q_3, r_3 \in \mathbb{Z}$$

$$...r_N = r_{N+1} q_{N+2} + 0, \text{ for some } q_{N+2}, r_{N+1} \in \mathbb{Z}$$

Clearly, $(a_{n-1}, a_n) \to (a_{n-1}, r_1) \to (r_2, r_1) \to (r_2, r_3).... \to (r_{N+1}, 0) = (gcd(a_{n-1}, a_n), 0)$. Moreover, (a_{n-2}, a_{n-1}, a_n) to $(\gcd(a_{n-2}, \gcd(a_{n-1}, a_n)), 0, 0)$. By iterations, $(a_1, a_2, a_3, ..., a_n)$ can be transformed to

$$(\gcd(a_1, \gcd(a_2, \gcd(a_3, ..., \gcd(a_{n-1}, a_n)))), 0, 0, ..., 0)$$

Since $\gcd(a_1, \gcd(a_2, \gcd(a_3, ..., \gcd(a_{n-1}, a_n)))) = 1$, then $(a_1, a_2, a_3, ..., a_n)$ can be transformed to $(1, 0, 0, ..., 0)$.