Set Theory (Math 111)
Final

Ali Nesin

January 11, 2004

You may assume that you know all the basic arithmetic properties of $(\mathbb{Z}, +, \times, 0, 1)$ and $(\mathbb{N}, +, \times, 0, 1)$.

1. *Let* $X = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. *Define the relation* $\equiv$ *on* X *by*

$$(x, y) \equiv (z, t) \Leftrightarrow xt = yz$$

for every (x, y), $(z, t) \in X$.

a) Show that this is an equivalence relation on X.

b) Find the equivalence classes of $(0, 1)$ *and of* $(3, 3)$.

c) Show that if $(x, y) \equiv (x', y')$ *and* $(z, t) \equiv (z', t')$ *then* $(xt + yz, yt) \equiv (x't' + y'z', y't')$.

d) Show that if $(x, y) \equiv (x', y')$ *and* $(z, t) \equiv (z', t')$ *then* $(xz, yt) \equiv (x'z', y't')$.

Proof: a. i. Reflexivity. Let $(x, y) \in X$. Then since $xy = yx$, we have $(x, y) \equiv (x, y)$.

ii. Symmetry. Let (x, y), $(z, t) \in X$ be such that $(x, y) \equiv (z, t)$. Hence $xt = yz$. Therefore $zy = tx$, implying $(z, t) \equiv (x, y)$.

iii. Transitivity. Let (x, y), (z, t), $(u, v) \in X$ be such that $(x, y) \equiv (z, t)$ and $(z, t) \equiv (u, v)$. Hence $xt = yz$ and $zv = tu$. Multiplying these equalities side by side, we get $xtzv = yztu$. Since $t \neq 0$, by simplifying we get $xzv = yzu$. If $z \neq 0$, then we can simplify further to get $xv = yu$, hence $(x, y) \equiv (u, v)$.

Assume $z = 0$. Then $xt = yz = 0$ and $tu = zv = 0$. Since $t \neq 0$, we get $x = u = 0$, so that $xv = 0 = yu$ and $(x, y) \equiv (u, v)$ again.

b. $\overline{(0, 1)} := \{(x, y) \in X : (x, y) \equiv (0, 1)\} = \{(x, y) \in X : x = 0\} = \{(0, y) : y \in \mathbb{Z} \setminus \{0\}\}$.

$\overline{(3, 3)} := \{(x, y) \in X : (x, y) \equiv (3, 3)\} = \{(x, y) \in X : 3x = 3y\} = \{(x, x) : x \in \mathbb{Z} \setminus \{0\}\}$.

c) Assume $(x,y) \equiv (x',y')$ and $(z,t) \equiv (z',t')$. Then $xy' = yx'$ and $zt' = tz'$. Multiplying the first one by tt' and the second one by yy' we get $xy'tt' = yx'tt'$ and $zt'yy' = tz'yy'$. Adding these two side by side we get $xy'tt' + zt'yy' = yx'tt' + tz'yy'$, and factoring, we get $(xt+yz)y't' = yt(x't'+y'z')$, meaning $(xt+yz, yt) \equiv (x't'+y'z', y't')$.

d) Assume $(x,y) \equiv (x',y')$ and $(z,t) \equiv (z',t')$. Then $xy' = yx'$ and $zt' = tz'$. Multiplying these two side by side, we get $xy'zt' = yx'tz'$, i.e. $xzy't' = ytx'z'$, meaning $(xz, yt) \equiv (x'z', y't')$.

2. *Find a graph which has only three automorphisms.*

   Solution. Consider the graph whose points are

   $$\{a,\, a',\, a'',\, a''',\, b,\, b',\, b'',\, b''',\, c,\, c',\, c'',\, c'''\}$$

   and whose vertices are

   $$aa',\, aa'',\, a''a''',\, bb',\, bb'',\, b''b''',\, cc',\, cc'',\, c''c''',\, ab,\, bc,\, ca,\, a'b'',\, b'c'',\, c'a''.$$

   It works!

3. *Let a and b be two integers which are not both 0. We say that d is the* **greatest common divisor** *of a and b if d is the largest natural number that divides both a and b. Show that for any a, $b \in \mathbb{Z}$, $\gcd(a,b)$ exists and that there are x, $y \in \mathbb{Z}$ such that $ax + by = \gcd(a,b)$.*

   Proof: Replacing a and b by $|a|$ and $|b|$, we may assume that $a \geq 0$ and $b \geq 0$.

   Existence. Since 1 divides both a and b and since any number that divides both a and b can be at most $\max(a,b) > 0$, the set of natural numbers that divide both a and b is a finite nonempty set bounded by $\max(a,b)$. Therefore there is a largest such number. This proves the existence of $\gcd(a,b)$. We let $d = \gcd(a,b)$.

   Second Part. We proceed by induction on $\max(a,b)$. If $a = 1$, then take $x = 1$, $y = 0$. If $b = 1$, then take $x = 0$, $y = 1$. This takes care of the initial step $\max(a,b)$. Assume $\max(a,b) > 1$. If $a = b$, then $d = a$ and we may take $x = 1$, $y = 0$. Assume $a \neq b$. Without loss of generality, we may assume that $a > b$. Note that the divisors of a and b are the same as the divisors of $a-b$ and b. Hence $\gcd(a-b, b) = \gcd(a,b) = d$. Since $\max(a-b,b) < a = \max(a,b)$, by induction there are two integers x and y' such that $x(a-b) + y'b = d$, i.e. $xa + (y'-x)b = d$. Take $y = y' - x$.

4. *Let a and b be two nonzero integers. We say that m is the* **least common multiple** *of a and b if m is the least natural number that is divisible by both a and b. We let $m = \operatorname{lcm}(a,b)$. Show that for any a, $b \in \mathbb{Z} \setminus \{0\}$, $\operatorname{lcm}(a,b)$ exists and that $ab = \pm \gcd(a,b) \operatorname{lcm}(a,b)$.*

Proof: Replacing a and b by $|a|$ and $|b|$ again, we may assume that $a > 0$ and $b > 0$. Since a and b both divide ab, $\mathrm{lcm}(a, b)$ exists.

Let $d = \gcd(a, b)$ and $m = \mathrm{lcm}(a, b)$. Let a' and b be such that $a = da'$ and $b = db'$. Then $ab = d^2a'b'$. We need to prove that $m = da'b'$.

Since $da'b' = ab' = a'b$, a and b both divide $da'b'$.

Let x be divisible by both a and b. Then $x = au = bv$ for some u, v. We have $a'du = au = x = bv = b'dv$ and so $a'u = b'v$. Since a' and b' cannot have a common divisor (otherwise d would be larger), b' must divide u. (This last fact needs a serious proof, that we have not undertaken yet. I shouldn't have asked this question at this stage). Write $u = cb'$. Now $x = au = acb' = a'dcb'$ and so $a'b'd$ divides x, in particular $a'b'd \leq x$. This shows that $a'b'd$ is the least multiple of a and b, i.e. $a'b'd = m$.

5. *Find formulas for the sums*

$$1^2 + 2^2 + \ldots + n^2$$

and

$$1^3 + 2^3 + \ldots + n^3,$$

and prove your result.

Proof: We claim that

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

We proceed by induction on n. For $n = 1$, it is easy to check the validity of the formula. Assume the statement holds for n. To prove it for $n + 1$, we compute:

$$\begin{aligned} 1^2 + 2^2 + \ldots + n^2 + (n+1)^2 &= \tfrac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \tfrac{(n+1)(n(2n+1)+6(n+1))}{6} \\ &= \tfrac{(n+1)(2n^2+7n+6))}{6} \\ &= \tfrac{(n+1)(n+2)(2n+3)}{6} \\ &= \tfrac{n'(n'+1)(2n'+1)}{6} \end{aligned}$$

where $n' = n + 1$. This proves the equality by induction.

We claim that

$$1^3 + 2^3 + \ldots + n^3 = \frac{n^2(n+1)^2}{4}.$$

We proceed by induction on n. For $n = 1$, it is easy to check the validity of the formula. Assume the statement holds for n. To prove it for $n + 1$, we compute:

$$\begin{aligned} 1^3 + 2^3 + \ldots + n^3 + (n+1)^3 &= \tfrac{n^2(n+1)^2}{4} + (n+1)^3 \\ &= \tfrac{(n+1)^2(n^2+4n+4)}{4} \\ &= \tfrac{(n+1)^2(n+2)^2}{4} \\ &= \tfrac{m^2(m+1)^2}{4} \end{aligned}$$

where $m = n + 1$. This proves the equality by induction.

6. *Recall that a natural number $p \neq 0,\, 1$ is called* **prime** *if whenever p divides a product xy of two natural numbers x and y then p divides either x or y. A natural number $p \neq 0,\, 1$ is called* **irreducible** *if whenever $p = xy$ for two natural numbers x and y then either x or y is 1. Show that a natural number is prime if and only if it is irreducible.*

   Proof: Let p be prime. Assume that $a|p$. Then $p = ab$ for some b. It follows that p divides ab. Thus p divides either a or b. Assume – without loss of generality – that p divides a. Then $px = a$ some x. Hence $p = ab = pxb$. Since $p \neq 0$, it follows that $xb = 1$. Thus $b = 1$, and so $a = p$.

   Let now p be an irreducible. We will prove that p is a prime. Let p divide xy. We will show that p divides either x or y. We proceed by induction on $p+x+y$. Dividing x and y by p we get $x = pq_1+x_1$ and $y = pq_2+y_1$ where $x_1,\, y_1 < p$. Since $xy = (pq_1+x_1)(pq_2+y_1) = p(pq_1q_2+q_1y_1+q_2x_1)+x_1y_1$, thus p divides x_1y_1. Assume $x_1y_1 \neq 0$. Thus $p \leq x_1y_1 < p^2$. It follows that $x_1y_1 = rp$ for some $r = 1, \ldots, p-1$. If $r = 1$, then either $p = x_1$ or $p = y_1$, a contradiction. Let q be an irreducible dividing r. Thus $q \leq r < p$. By induction q divides either x_1 or y_1, say q divides x_1. Write $x_1 = qx_2$ and $r = qr'$. We have $qx_2y_1 = x_1y_1 = rp = qr'p$ and $x_2y_1 = r'p$. By induction p divides either x_2 or y_1, in which case it divides x or y (respectively). Thus we may assume that $x_1y_1 = 0$. Hence one of x_1 or y_1 is 0, say $x_1 = 0$. Then $x = pq_1 + x_1 = pq_1$ and p divides x. $\square$