

1ST MIDTERM, MATH 441 - OCTOBER 11, 2005

NIGEL BOSTON

1. Define a relation \sim on the set of real numbers \mathbf{R} by saying that $x \sim y$ if and only if $x - y$ is an integer. Is this relation an equivalence relation? If so, describe the equivalence class that contains 0.5 and describe the partition of \mathbf{R} produced by the equivalence relation.

2. Show that every integer x satisfies $x^3 \equiv x \pmod{3}$. Show by induction that $x^{3^n} \equiv x \pmod{3}$. What is the remainder on dividing 2^{28} by 3? (There is a quick way.)

3. Show that $\sqrt{3}$ is not a rational number. Let $\mathbf{Q}[\sqrt{3}]$ consist of all real numbers of the form $a + b\sqrt{3}$, where a, b are any rational numbers. You may assume that $\mathbf{Q}[\sqrt{3}]$ is a ring. Assuming this, is it true that $\mathbf{Q}[\sqrt{3}]$ is a field?

4. Find integers r, s such that $1 = 11r + 13s$. Find an integer x satisfying $11x \equiv 3 \pmod{13}$. What are the units of $\mathbf{Z}/13\mathbf{Z}$?

(1) Need to check R,S,T.

R holds since $x - x$ is an integer for every x in \mathbf{R} . S holds since if $x - y$ is an integer, say n , then $y - x$ is an integer, namely $-n$. T holds since if $x - y$ and $y - z$ are integers, then $x - z = (x - y) + (y - z)$ is also an integer.

$x - 0.5$ is an integer if x is an integer plus a half, so the equivalence class is $\{\dots, -0.5, 0.5, 1.5, 2.5, \dots\}$.

Likewise a typical subset in the partition is $\{\dots, -1 + a, a, 1 + a, 2 + a, \dots\}$ where a can be chosen in $[0, 1)$.

(2) If $x \equiv 0, 1, 2 \pmod{3}$, then $x^3 \equiv 0, 1, 2 \pmod{3}$ respectively, so $x^3 \equiv x \pmod{3}$.

Let $P(n)$ be the statement $x^{3^n} \equiv x \pmod{3}$. We just showed $P(1)$. Now assume $P(n)$ is true. Look at $x^{3^{n+1}} = (x^{3^n})^3$. This $\equiv x^3$ by $P(n)$. But by what we just showed, this $\equiv x \pmod{3}$. So $P(n+1)$ is established. That completes the induction.

By what we just showed, $2^{27} \equiv 2 \pmod{3}$ and so $2^{28} \equiv 4 \equiv 1 \pmod{3}$, so the remainder is 1.

(3) Suppose $\sqrt{3} = a/b$ where a, b are positive integers. Then $3 = a^2/b^2$, so $a^2 = 3b^2$. The power of 3 dividing a^2 must be even, whereas the power of 3 dividing $3b^2$ is odd. A contradiction, so $\sqrt{3}$ is not rational.

Let $a + b\sqrt{3}$ be a nonzero element. Then $\frac{1}{a+b\sqrt{3}} = \frac{(a-b\sqrt{3})}{(a+b\sqrt{3})(a-b\sqrt{3})} = \frac{a-b\sqrt{3}}{a^2-3b^2} = \frac{a}{a^2-3b^2} + \frac{-b}{a^2-3b^2}$ so every nonzero element is a unit, so $\mathbf{Q}[\sqrt{3}]$ is a field.

(4) $13 = 1 * 11 + 2, 11 = 5 * 2 + 1$, so $1 = 11 - 5 * 2 = 11 - 5 * (13 - 11) = 6 * 11 - 5 * 13$ (\dagger), so take $r = 6, s = -5$. Taking (\dagger) mod 13, $1 \equiv 6 * 11 \pmod{13}$. Multiplying by 3, $3 \equiv 18 * 11 \pmod{13}$. So $x = 18$ works. Since 13 is prime, every nonzero element of $\mathbf{Z}/13\mathbf{Z}$ is a unit.