(*January 14, 2009*)

[01.1] Let D be an integer that is not the square of an integer. Prove that there is no $\sqrt{D}$ in $\mathbb{Q}$.

Suppose that a, b were integers ($b \neq 0$) such that $(a/b)^2 = D$. The fact/principle we intend to invoke here is that fractions can be put in *lowest terms*, in the sense that the numerator and denominator have greatest common divisor 1. This follows from *existence* of the *gcd*, and from the fact that, if $\gcd(a,b) > 1$, then let $c = a/\gcd(a,b)$ and $d = b/\gcd(a,b)$ and we have $c/d = a/b$. Thus, still $c^2/d^2 = D$. One way to proceed is to prove that c^2/d^2 is still in lowest terms, and thus cannot be an integer unless $d = \pm 1$. Indeed, if $\gcd(c^2, d^2) > 1$, this *gcd* would have a prime factor p. Then $p|c^2$ implies $p|c$, and $p|d^2$ implies $p|d$, by the critical proven property of primes. Thus, $\gcd(c,d) > 1$, contradiction.

[01.2] Let p be prime, $n > 1$ an integer. Show (directly) that the equation $x^n - px + p = 0$ has no rational root (where $n > 1$).

Suppose there were a rational root a/b, without loss of generality in lowest terms. Then, substituting and multiplying through by b^n, one has

$$a^n - pb^{n-1}a + pb^n = 0$$

Then $p|a^n$, so $p|a$ by the property of primes. But then p^2 divides the first two terms, so must divide pb^n, so $p|b^n$. But then $p|b$, by the property of primes, contradicting the lowest-common-terms hypothesis.

[01.3] Let p be prime, b an integer not divisible by p. Show (directly) that the equation $x^p - x + b = 0$ has no rational root.

Suppose there were a rational root c/d, without loss of generality in lowest terms. Then, substituting and multiplying through by d^p, one has

$$c^p - d^{p-1}c + bd^p = 0$$

If $d \neq \pm 1$, then some prime q divides d. From the equation, $q|c^p$, and then $q|c$, contradiction to the lowest-terms hypothesis. So $d = 1$, and the equation is

$$c^p - c + b = 0$$

By Fermat's Little Theorem, $p|c^p - c$, so $p|b$, contradiction.

[01.4] Let r be a positive integer, and p a prime such that $\gcd(r, p-1) = 1$. Show that every b in $\mathbb{Z}/p$ has a unique r^{th} root c, given by the formula

$$c = b^s \bmod p$$

where $rs = 1 \bmod (p-1)$. [*Corollary of Fermat's Little Theorem.*]

[01.5] Show that $R = \mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ are Euclidean.

First, we consider $R = \mathbb{Z}[\sqrt{-D}]$ for $D = 1, 2, \ldots$. Let $\omega = \sqrt{-D}$. To prove Euclidean-ness, note that the Euclidean condition that, given $\alpha \in \mathbb{Z}[\omega]$ and non-zero $\delta \in \mathbb{Z}[\omega]$, there exists $q \in \mathbb{Z}[\omega]$ such that

$$|\alpha - q \cdot \delta| < |\delta|$$

is equivalent to

$$|\alpha/\delta - q| < |1| = 1$$

Thus, it suffices to show that, given a complex number α, there is $q \in \mathbb{Z}[\omega]$ such that

$$|\alpha - q| < 1$$

Every complex number α can be written as $x + y\omega$ with real x and y. The simplest approach to analysis of this condition is the following. Let m, n be integers such that $|x - m| \leq 1/2$ and $|y - n| \leq 1/2$. Let $q = m + n\omega$. Then $\alpha - q$ is of the form $r + s\omega$ with $|r| \leq 1/2$ and $|s| \leq 1/2$. And, then,

$$|\alpha - q|^2 = r^2 + Ds^2 \leq \frac{1}{4} + \frac{D}{4} = \frac{1+D}{4}$$

For this to be strictly less than 1, it suffices that $1 + D < 4$, or $D < 3$. This leaves us with $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-2}]$.

In the second case, consider $Z[\omega]$ where $\omega = (1 + \sqrt{-D})/2$ and $D = 3 \bmod 4$. (The latter condition assures that $\mathbb{Z}[x]$ works the way we hope, namely that everything in it is expressible as $a + b\omega$ with $a, b \in \mathbb{Z}$.) For D=3 (the Eisenstein integers) the previous approach still works, but fails for $D = 7$ and for $D = 11$. Slightly more cleverly, realize that first, given complex α, integer n can be chosen such that

$$-\sqrt{D}/4 \le \text{imaginary part}(\alpha - n\omega) \le +\sqrt{D}/4$$

since the imaginary part of ω is $\sqrt{D}/2$. *Then* choose integer m such that

$$-1/2 \le \text{ real part}(\alpha - n\omega - m) \le 1/2$$

Then take $q = m + n\omega$. We have chosen q such that $\alpha - q$ is in the *rectangular* box of complex numbers $r + s\sqrt{-7}$ with

$$|r| \le 1/2 \quad \text{and} \quad |s| \le 1/4$$

Yes, 1/4, not 1/2. Thus, the size of $\alpha - q$ is at most

$$1/4 + D/16$$

The condition that this be strictly less than 1 is that $4 + D < 16$, or $D < 12$ (and $D = 1 \bmod 4$). This gives $D = 3, 7, 11$.

[01.6] Let $f : X \to Y$ be a function from a set X to a set Y. Show that f has a left inverse if and only if it is injective. Show that f has a right inverse if and only if it is surjective. (Note where, if anywhere, the Axiom of Choice is needed.)

[01.7] Let $h : A \to B$, $g : B \to C$, $f : C \to D$. Prove the associativity

$$(f \circ g) \circ h = f \circ (g \circ h)$$

Two functions are equal if and only if their values (for the same inputs) are the same. Thus, it suffices to evaluate the two sides at $a \in A$, using the definition of composite:

$$((f \circ g) \circ h)(a) = (f \circ g)(h(a)) = f(g((h(a))) = f((g \circ h)(a)) = (f \circ (g \circ h))(a)$$

[01.8] Show that a set is infinite if and only if there is an injection of it to a proper subset of itself. Do not set this up so as to trivialize the question.

The other definition of *finite* we'll take is that a set S is finite if there is a surjection to it from one of the sets

$$\{\},\ \{1\},\ \{1,2\},\ \{1,2,3\},\ \ldots$$

And a set is *infinite* if it has no such surjection.

We find a denumerable subset of an infinite set S, as follows. For infinite S, since S is not empty (or there'd be a surjection to it from $\{\}$), there is an element s_1. Define

$$f_1 : \{1\} \to S$$

by $f(1) = s_1$. This cannot be surjective, so there is $s_2 \ne s_1$. Define

$$f_2 : \{1,2\} \to S$$

by $f(1) = s_1$, $f(2) = s_2$. By induction, for each natural number n we obtain an injection $f_n : \{1, \ldots\} \to S$, and distinct elements $s_1, 2_2, \ldots$. Let S' be the complement to $\{s_1, s_2, \ldots\}$ in S. Then define $F : S \to S$ by

$$F(s_i) = s_{i+1} \quad F(s') = s' \text{ (for } s' \in S')$$

This is an injection to the proper subset $S - \{s_1\}$.

On the other hand, we claim that no set $\{1, \ldots, n\}$ admits an injection to a proper subset of itself. If there were such, by Well-Ordering there would be a least n such that this could happen. Let f be an injection of $S = \{1, \ldots, n\}$ to a proper subset of itself.

By hypothesis, f restricted to $S' = \{1, 2, \ldots, n-1\}$ does *not* map S' to a proper subset of itself. The restriction of an injective function is still injective. Thus, either $f(i) = n$ for some $1 \leq i < n$, or $f(S')$ is the *whole* set S'. In the former case, let j be the least element not in the image $f(S)$. (Since $f(i) = n$, $j \neq n$, but this doesn't matter.) Replace f by $\pi \circ f$ where π is the permutation of $\{1, \ldots, n\}$ that interchanges j and n and leaves everything else fixed. Since permutations are bijections, this $\pi \circ f$ is still an injection of S to a proper subset. Thus, we have reduced to the second case, that $f(S') = S'$. By injectivity, $f(n)$ can't be in S', but then $f(n) = n$, and the image $f(S)$ is not a proper subset of S after all, contradiction. ///

In a similar vein, one can *prove* the Pigeon-Hole Principle, namely, that for $m < n$ a function

$$f : \{1, \ldots, n\} \to \{1, \ldots, m\}$$

cannot be injective. Suppose this is false. Let n be the smallest such that there is $m < n$ with an injective map as above. The restriction of an injective map is still injective, so f on $\{1, \ldots, n-1\}$ is still injective. By the minimality of n, it must be that $n - 1 = m$, and that f restricted to $\{1, \ldots, m\}$ is a bijection of that set to itself. But then there is no possibility for $f(n)$ in $\{1, \ldots, m\}$ without violating the injectivity. Contradiction. Thus, there is no such injection to a smaller set.