Modular Arithmetic

Tim Smits

1. A *prime triplet* is a pair $(p, p+2, p+4)$ where p is a prime number. Prove $(3, 5, 7)$ is the only prime triplet. (The question of how many prime *pairs* there are is a very hard open problem!).

2. Show that the equation $15x^2 - 7y^2 = 9$ has no integer solutions.

3. Show that none of the integers in the sequence $11, 111, 1111, 11111, 111111, \ldots$ is a perfect square.

4. (a) (Fermat's Little Theorem) Let p be a prime. Prove that $[a]^{p-1} = [1]$ for any non-zero $[a] \in \mathbb{Z}/p\mathbb{Z}$. (Hint: show that $[x] \to [a][x]$ is a bijection).

   (b) (Wilson's Theorem) Prove that n is prime if and only if $(n-1)! \equiv -1 \bmod n$.

Solutions

The first three problems all illustrate a very powerful technique for solving problems in the integers: work modulo n instead!

1. Case on the value of $p \bmod 3$: If $p \equiv 0 \bmod 3$, then $p = 3$ and we get the triple $(3, 5, 7)$. Otherwise, if $p \equiv 1 \bmod 3$ then $p + 2 \equiv 0 \bmod 3$ says $p + 2 = 3$, so $p = 1$, which is not prime. If $p \equiv 2 \bmod 3$, then $p + 4 \equiv 0 \bmod 3$ says $p + 4 = 3$, and -1 is not prime.

2. If $15x^2 - 7y^2 = 9$ had integer solutions, then taking this mod 15 says the equation $8y^2 = 9 \bmod 15$ has solutions, or $y^2 = 3 \bmod 15$ after multiplying by 2. One can check directly however that $[3]$ is not a square in $\mathbb{Z}/15\mathbb{Z}$, a contradiction. Therefore, no integer solutions exist.

3. Explicitly, the sequence is given by $a_n = \frac{1}{9}(10^{n+1} - 1)$ for $n \geq 1$. Suppose for contradiction that $a_n = x^2$ for some integers x and n. Since $9 \equiv 1 \bmod 4$, we have $\frac{1}{9} \equiv 1 \bmod 4$, so this says that $a_n \equiv 2^{n+1} - 1 \bmod 4 \equiv 3 \bmod 4$, as $4 \mid 2^{n+1}$ for $n \geq 1$. However, note that $x^2 \equiv 3 \bmod 4$ has no solutions, so a_n cannot be a perfect square.

4. (a) For $[a] \neq [0] \in \mathbb{Z}/p\mathbb{Z}$, define a function $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ by $f([x]) = [a][x]$. I claim that f is injective. Suppose that $f([x]) = f([y])$ for some $[x], [y] \in \mathbb{Z}/p\mathbb{Z}$. Then $[a][x] = [a][y]$ so $[a]([x] - [y]) = [0]$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, multiplying by $[a]^{-1}$ says $[x] - [y] = [0]$, so $[x] = [y]$. Therefore f is injective, and since f is a map from a finite set to itself, it's therefore bijective. Therefore, the set $\{[a], [2a], [3a], \ldots, [(p-1)a]\}$ must be a permutation of the set $\{[1], [2], \ldots, [p-1]\}$. Taking the product of all elements in each set, we find $[a]^{p-1} \prod_i [i] = \prod_i [i]$. Note that $[i] \in \mathbb{Z}/p\mathbb{Z}$ is a unit for $i \neq 0$, and the product of units is still a unit. Therefore, we can cancel $\prod_i [i]$ from both sides to conclude that $[a]^{p-1} = [1]$.

   (b) First assume that $n = p$ is prime. Then we want to show that $(p-1)! \equiv -1 \bmod p$. The trick is to observe that since $\mathbb{Z}/p\mathbb{Z}$ is a field, every non-zero element $[a] \in \mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse. Therefore, every element in $\prod [i]$ pairs up with it's inverse to make $[1]$. The only exceptions are $[1]$ and $[p-1]$, because these are the only solutions to $[x]^2 = [1]$ (i.e. the elements who are their own multiplicative inverse). This says that $\prod_i [i] = [p-1]$, or in otherwords, $(p-1)! \equiv -1 \bmod p$. If n is not prime, write $n = ab$ for some $1 < a, b < n$. Then a, b both appear as terms in $(n-1)!$, so $(n-1)! \equiv 0 \bmod n$.