Lisbon Summer School (2011) Problem Set 1

Christopher Skinner

These exercises vary in difficulty and importance. Try the ones that interest you.

1. Let p be a prime number (that is, a positive prime in $\mathbf{Z}$). Let n be a positive integer and $d = \gcd(n, p-1)$.

   a) Explain why the number of solutions to $x^n \equiv 1 \bmod p$ in $\mathbf{Z}/p$ is d.

   b) For any $a \not\equiv 0 \bmod p$, show that the number of solutions to $x^n \equiv a \bmod p$ in $\mathbf{Z}/p$ is either 0 or d.

2. Let p be a prime number.

   a) Show that if p is a sum of two squares (i.e., $p = x^2 + y^2$ for some $x, y \in \mathbf{Z}$) then $p = 2$ or $p \equiv 1 \bmod 4$ (i.e., $p = 4k+1$ for some integer k). In the rest of this exercise you will prove the converse.

   b) Given any $a \in \mathbf{Z}$ such that $p \nmid a$, show that there exist integers $x, y \in \{1, \ldots, [\sqrt{p}]\}$ such that either $ax \equiv y \bmod p$ or $ax \equiv -y \bmod p$. Hint: Consider all sums $au + v$ with $u, v \in \{0, \ldots, [\sqrt{p}]\}$; deduce that two of them must be congruent modulo p.

   c) If $p \equiv 1 \bmod 4$ apply the result of b) using an integer a such that $a^2 \equiv -1 \bmod p$ to prove that there exist integers $x, y \in \{1, \ldots, [\sqrt{p}]\}$ such that $x^2 + y^2 \equiv 0 \bmod p$. Conclude that $p = x^2 + y^2$.

3. a) Show that there is no solution in $\mathbf{Z}/7$ to $x^2 - 6x + 4 \equiv 0 \bmod 7$.

   b) Do there exist $x, y \in \mathbf{Z}$ such that $x^2 - 6xy + 4y^2 = 7$?

4. Fill in any details of the proof of the Chevalley-Warning theorem not done in lecture. Extend the theorem to show that the number of simultaneous solutions of

$$F_1(x_1, \ldots, x_s) \equiv 0 \bmod p, \quad F_2(x_1, \ldots, x_s) \equiv 0 \bmod p, \quad \ldots \quad , F_r(x_1, \ldots, x_s) \equiv 0 \bmod p$$

   in $\mathbf{Z}/p$ is divisible by p if

$$s > \deg(F_1) + \deg(F_2) + \cdots + \deg(F_r).$$

5. Find the solutions to $x^2 \equiv -1 \bmod 5^5$ and $x^2 \equiv -1 \bmod 11^3$.

6. Let p be an odd prime number.

   a) Show that for each $k \geq 1$ there are $p-1$ solutions in $\mathbf{Z}/p^k$ to $x^{p-1} \equiv 1 \bmod p^k$ and that for any such solution $x \bmod p^k$ its order mod p^k is the same as the order of $x \bmod p$. (For example, if $x \bmod p^k$ satisfies $x^{p-1} \equiv 1 \bmod p^k$ and has order 6 then $x \bmod p$ has order 6).

   b) Let $w \in \mathbf{Z}/p^k$ satisfy $w^{p-1} \equiv 1 \bmod p^k$ and have order $p-1$ (why does such w exist?). Show that $g = w(1+p)$ has order $p^{k-1}(p-1)$ in $\mathbf{Z}/p^k$. That is, $g^{p^{k-1}(p-1)} \equiv 1 \bmod p^k$ and $g^j \not\equiv 1 \bmod p^k$ for $1 \leq j < p^{k-1}(p-1)$. Thus $(\mathbf{Z}/p^k)^\times$ is a cyclic group with generator g.

c) What happens in part b) for $p = 2$?

7. Let $f(x, y) = y^2 - x^3 + 51$. The point $(1375/9, 50986/27) \in \mathbf{Q}^2$ is a solution to $f(x, y) = 0$. Show that $f(x, y) \equiv 0 \bmod p^k$ has solutions for every prime p and every $k \geq 1$. Hint: if $p \neq 3$ then use the given rational solution to produce a solution mod p^k. If $p = 3$ then use Hensel's lemma to show that $y^2 + 50 \equiv 0 \bmod 3^k$ has a solution for all $k \geq 1$