C. SKINNER class 1

11 de Julho de 2011

The Diophatine Problem: Given a polynomial $F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ are there elements $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ such that $F(\mathbf{a}) = 0$?
We can replace $\mathbb{Z}$ with another ring and ask the same question there.

If $F(\mathbf{a}) = 0$ then $F(\mathbf{a}) \equiv 0 \mod (N)$ por every $N \in \mathbb{N}$. So solving this equation for every N is a necessary condition for having an integer solution.

Examples:

1. Working modulo 3 we find that the equation $x^2 - 3y^2 = 2$ has no solution since $x^2 \equiv 2 \mod (3)$ is impossible.

2. For the equation $x^2 - 3y^2 = 7$ working modulo 3 does not work. Working modulo 4 we get $x^2 + y^2 \equiv 3$. So there is no solutions because $x^2, y^2 \equiv 0, 1 \mod (4)$.

Chinese Remainder Theorem (CRT): If $N = N_1 \cdots N_r$ and $\gcd(N_i, N_j) = 1$ when $i \neq j$ then $\mathbb{Z}_n \cong Z_{N_1} \times \ldots \times \mathbb{Z}_{N_r}$. The isomorphism is given by $a \mod N \mapsto (a \mod N_1, \ldots, a \mod N_r)$.

By the CRT, to have a solution modulo every N, it is enough to have a solution modulo all prime powers p^k. For this reason we will study this king of congruences, starting with the case $k = 1$.
We know that $\mathbb{Z}_p$ is a field. Denote by U_p the group of units of $\mathbb{Z}_p$ (i.e, $U_p = \{1, \ldots, p-1\}$). Given $x \in U_p$ we define $\psi : Z_p \to Z_p$ such that $\psi(a) = ax$. It is easy to see that ψ is a morphism. Indeed, ψ is a monomorphism. If $ax \equiv 0 \mod (p)$, since Z_p is an Integral Domain, then $a \equiv 0 \mod (p)$ or $x \equiv 0 \mod (p)$ and by hypothesis we conclude that $a \equiv 0 \mod (p)$. This means that $ker\phi = \{0\}$ and so ϕ is a monomorphism.

Claim: U_p is a cyclic group.

Proof:
An as abstract group we have that $U_p \cong \mathbb{Z}_{q_1{}^{a_1}} \times \ldots \times \mathbb{Z}_{q_r{}^{a_r}}$. If $q_1 = q_2$ then there are at least q^2 elements of order q in U_p. But this cannot happen since it would give q^2 roots of $x^q - 1 \in \mathbb{Z}_p[x]$ wich is impossible because $\mathbb{Z}_p$ is an

Integral Domain.

A generator of U_p is called a primitive root modulo p. Suppose a is a solution to $x^2 \equiv -1 \mod (p)$. Then if $a^2 \neq 1$ in U_p we have that $a^4 \equiv 1$. This means that a as order 4 in U_p wich happens if and only if $4|p-1$. In this case, $a = g^{\frac{p-1}{4}}$ for a primitive root g of U_p.

Chevalley-Warning Theorem:
Let $F(x_1, \ldots, x_s) \in \mathbb{Z}_p[x_1, \ldots, x_s]$. If $s > \deg F$ then $p|\#\{\mathbf{a} \in {\mathbb{Z}_p}^s : F(\mathbf{a}) = 0\}$.
Example: Let $F(x, y, z) = ax^2 + by^2 + cz^2$. We have $\deg F = 2$ and the numbers of variables is $s = 3 > 2$. By the above theorem, since every prime p is bigger than 1 and $(0, 0, 0)$ is a solution, there must be another solution.

Lemma:
Let $r \geq 0$ be an integer. Then

$$\sum_{x \in Z_p} x^r = \begin{cases} p-1 & \text{if } p-1|r \\ 0 & \text{otherwise} \end{cases}$$

Proof:
Leg g be a primitive root in U_p. Then

$$\sum_{x \in Z_p} x^r = \sum_{x \in U_p} x^r = \sum_{i=0}^{p-2} g^{ir}$$

If $p-1 \not| r$ then, by the geometric sum formula, this evaluates toi 0. Otherwise, $g^{ir} = 1$ for $i = 0, \ldots, p-2$ and we get $p-1$ as the value of the sum.