1. Solutions to homogeneous linear congruences

The focus of Math 104C will be the study of quadratics.

The first problem we will consider is representation of integers as sums of squares. We start with some explicit bounds on the solutions to systems of homogeneous linear congruences.

Theorem 1.1 (Brauer-Reynolds)**.** *Let r, s and m be natural numbers, and let $\lambda_1, \lambda_2, \ldots, \lambda_s$ be positive real numbers such that*

$$\lambda_1 < m, \ldots, \lambda_s < m \qquad \text{and} \qquad \lambda_1 \lambda_2 \ldots \lambda_s > m^r,$$

so that in particular $m > 1$ and $r < s$.

Then the $r \times s$ system of homogeneous linear congruences

$$\sum_{j=1}^{s} a_{ij} x_j \equiv 0 \mod m,$$

where $1 \leq i \leq r$ and $a_{ij} \in \mathbb{Z}$ has a solution $u_1, u_2, \ldots, u_s$, not all zero modulo m, such that $|u_i| < \lambda_i$, for $1 \leq j \leq s$.

Proof. If we perturb $\lambda_1, \lambda_2, \ldots, \lambda_r$ a little bit by decreasing them, whilst preserving the condition that

$$\lambda_1 \lambda_2 \ldots \lambda_s > m^r,$$

we may assume that none of them are integers.

Let

$$\sum_{j=1}^{s} a_{ij} x_j = y_i.$$

Suppose that

$$0 \leq x_j \leq \llcorner \lambda_j \lrcorner.$$

We get $1 + \llcorner \lambda_j \lrcorner$ possible values for x_j and since $\lambda_j \leq m$ these give distinct values modulo m. Thus there are

$$l = \prod_{j=1}^{s} (1 + \llcorner \lambda_j \lrcorner)$$

different s-tuples $(x_1, x_2, \ldots, x_s)$ modulo m.

Each such s-tuple gives rise to an r-tuple $(y_1, y_2, \ldots, y_r)$ of which there are m^r modulo m. As

$$\begin{aligned} l &> \lambda_1 \lambda_2 \ldots \lambda_s \\ &> m^r. \end{aligned}$$

we may apply the pigeonhole principle. It follows that there are two s-tuples $(x_1, x_2, \ldots, x_s)$ and $(x'_1, x'_2, \ldots, x'_s)$ which are not equal modulo m and which give rise to the same r-tuple $(y_1, y_2, \ldots, y_r)$. As we have

linear homogeneous equations the difference $(u_1 = x_1 - x_1', u_2 = x_2 - x_2', \dots, u_s = x_s - x_s')$ is a solution of the original linear homogeneous equations modulo m.

As $(x_1, x_2, \dots, x_s)$ and $(x_1', x_2', \dots, x_s')$ are not equal modulo m it follows that at least one u_j is non-zero modulo m. Finally note that

$$|u_j| < \lambda_j. \qquad \square$$

Corollary 1.2 (Aubry, Thue, Vinogradov)**.** *If $1 < \lambda < m$ is a real then for every a not divisible by m we may find x and y such that*

$$ax \equiv y \mod m$$

where $1 \le x < \lambda$ and $1 \le |y| \le m/\lambda$.

Proof. Pick $\epsilon > 0$ sufficiently small. Then $1 < (1-\epsilon)\lambda < m$. Moreover as y is an integer it follows that

$$|y| < \frac{m}{(1-\epsilon)\lambda} \qquad \text{implies} \qquad |y| \le \frac{m}{\lambda}.$$

Let

$$\mu = \frac{m}{(1-\epsilon)\lambda}.$$

We apply (1.1) with $r = 1$, $s = 2$, $a_{11} = a$, $a_{12} = -1$, $\lambda_1 = \lambda$ and $\lambda_2 = \mu$. Note that $\mu < m$ as $(1-\epsilon)\lambda > 1$ and

$$\begin{aligned} \lambda\mu &= \lambda \frac{m}{(1-\epsilon)\lambda} \\ &= \frac{m}{(1-\epsilon)} \\ &> m. \end{aligned}$$

We get u and v, not both zero modulo m, such that

$$au - y \equiv 0 \mod m$$

and $0 \le |u| < \lambda$, $0 \le |v| < \mu$. As we already reasoned, it follows that $0 \le |v| \le m/\lambda$. If one of u or v is zero modulo m then so is the other and so we may assume that u are v are both non-zero modulo m. Finally, possibly replacing (u, v) by $(-u, -v)$ we may assume that $u > 0$, so that $1 \le u < \lambda$ and $1 \le |v| \le m/\lambda$. $\square$

Theorem 1.3. *Let p be a prime and let k be a natural number.*
Suppose that either

(1) k is odd and $(k, p-1) = d > 1$, or
(2) $k = 2$ and $p \equiv 1 \mod 4$.

Then there is a natural number $0 < n_k < \sqrt{p}$ *such that the equation*

$$x^k \equiv n_k \mod p,$$

has no solutions.

Proof. The hypotheses guarantee that we may find a such that

$$x^k \equiv a \mod p,$$

has no solutions and also that

$$x^k \equiv -1 \mod p,$$

has a solution.

Suppose that z is coprime to p. Then

$$x^k \equiv z \mod p$$

has a solution if and only if

$$x^k \equiv az \mod p$$

does not have a solution.

If we apply (1.2) then we get u and v such that $au \equiv v \mod p$, $1 \leq u < \sqrt{p}$ and $1 \leq |v| \leq \sqrt{p}$. Note that $\sqrt{p}$ is not an integer and so we may replace the last inequality with a strict inequality. At least one of u and v does not have a kth root modulo p. If it is not u and $v < 0$ then replace v by $-v$ and use the fact that -1 is a kth root. $\square$