Number Theory Solutions: Siegel's Ellipse

William F. Hammond

The following problem was on the last assignment:

> Can you find the smallest integer $m \geq 2$ with the property that there are *no* integers x, y for which
> $$5x^2 + 11y^2 \equiv 1 \pmod{m} \ ?$$

The answer to the question is "No" since there is no smallest such m. In other words, even though there is obviously no integer point on the ellipse

$$5x^2 + 11y^2 = 1$$

there are, for each modulus m, points (x, y) with integer coordinates for which the congruence mod m is satisfied. In fact, the mathematician C. L. Siegel (1896 – 1981) produced this as an example of an ellipse that for each modulus m is "equivalent" to the ellipse

$$x^2 + 55y^2 = 1 \quad .$$

Proof. To show the existence of solutions (x, y) mod m for each m it is enough by the Chinese Remainder Theorem to treat the case where m is the power of a prime.

If m is the power of an odd prime, or is any positive odd number, then, letting u_m be a multiplicative inverse of 4 mod m one has

$$5u_m^2 + 11u_m^2 \equiv 16u_m^2 \equiv 1 \pmod{m} \quad .$$

One then proceeds to treat the case $m = 2^n$, $n \geq 1$ recursive ly. Bear in mind that the value of an integer t mod 2^n determines the value of t^2 mod 2^{n+1}.

It is obvious that (x, y) is a solution mod 4 if and only if

$$x \equiv 1 \ \text{ and } \ y \equiv 0 \pmod{2}$$

since all odd squares are 1 mod 4.

However, $(1, 0)$ is not a solution mod 8. One sees that every solution mod 8 must be congruent to $(\pm 1, 2)$ mod 4, while $(\pm 1, \pm 2)$ and $(\pm 3, \pm 2)$ are all of the distinct solutions mod 8. Of the distinct solutions mod 8 only $(\pm 1, \pm 2)$ are solutions mod 16, while the distinct solutions mod 16 are $(\pm 1, \pm 2)$, $(\pm 7, \pm 2)$, $(\pm 1, \pm 6)$, and $(\pm 7, \pm 6)$. These observatio ns lead one to guess that there might be 2^n solutions mod 2^n for all $n \geq 1$.

Suppose that (x_n, y_n) is a solution mod 2^n for $n \geq 3$. Then there is an integer u_n such that

$$5x_n^2 + 11y_n^2 = 1 + 2^n u_n \ ,$$

and the validity of this relation depends only on (x_n, y_n) mod 2^{n-1}. If (x_{n+1}, y_{n+1}) is to be a solution mod 2^{n+1} that reduces mod 2^{n-1} to (x_n, y_n), then one must have

$$\begin{cases} x_{n+1} = x_n + 2^{n-1}s \\ y_{n+1} = y_n + 2^{n-1}t \end{cases}$$

for some integers s, t. Then let

$$u_{n+1} = \frac{5x_{n+1}^2 + 11y_{n+1}^2 - 1}{2^{n+1}} \quad .$$

u_{n+1} is certainly a rational number, and it is an integer if and only if $2^{n+1}u_{n+1} \equiv 0 \pmod{2^{n+1}}$.

After some computation one sees that the last condition becomes

$$2^n u_n + 2^n(5x_n s + 11y_n t) + 2^{2n-2}(\ldots) \equiv 0 \pmod{2^{n+1}}$$

which is equivalent to

$$u_n + 5x_n s + 11y_n t \equiv u_n + s \equiv 0 \pmod{2}$$

Thus, one has a solution (x_{n+1}, y_{n+1}) mod 2^{n+1} by choosing $s \equiv u_n$ mod 2 and t arbitarily. In fact, the free choice mod 2 for t is the reason why the number of solutions (x_n, y_n) mod 2^n is 2^n.