SQUARE APPLICATIONS, II

KEITH CONRAD

1. Introduction

We discuss here some applications of squares modulo primes to prove certain equations have no integral solutions because of congruence obstructions. A simple example of this idea is the equation $x^2 - 15y^2 = 7$. It has no integral solution because if it did then reduction of both sides modulo 5 implies $x^2 \equiv 2 \bmod 5$, but $2 \bmod 5$ is not a square. This contradiction shows $x^2 - 15y^2 = 7$ has no integral solutions. We say there is a congruence obstruction modulo 5.

Below we will see more subtle congruence obstructions to integral solvability of equations, putting to work some square patterns observed in numerical data:

$$\begin{aligned} -1 \equiv \Box \bmod p &\iff p = 2 \text{ or } p \equiv 1 \bmod 4, \\ 2 \equiv \Box \bmod p &\iff p = 2 \text{ or } p \equiv 1, 7 \bmod 8, \\ -2 \equiv \Box \bmod p &\iff p = 2 \text{ or } p \equiv 1, 3 \bmod 8. \end{aligned}$$

The equations we look at will all have the form $y^2 = x^3 + k$ for some constant k. Some equations have a $\mathbf{Z}$-solution by inspection (do you see an integral solution to $y^2 = x^3 - 26$?). If a search reveals no integral solutions with small x and y, one might hope to prove that no integral solution exists. Square patterns will be used in such proofs.

2. Examples

Theorem 2.1. *The equation $y^2 = x^3 - 5$ has no integral solutions.*

Proof. Assuming there is a solution, reduce modulo 4:

$$y^2 \equiv x^3 - 1 \bmod 4.$$

Here is a table of values of y^2 and $x^3 - 1$ modulo 4:

y	$y^2 \bmod 4$	x	$x^3 - 1 \bmod 4$
0	0	0	3
1	1	1	0
2	0	2	3
3	1	3	2

The only common value of $y^2 \bmod 4$ and $x^3-1 \bmod 4$ is 0, so by y is even and $x \equiv 1 \bmod 4$. Then rewrite $y^2 = x^3 - 5$ as

$$y^2 + 4 = x^3 - 1 = (x-1)(x^2 + x + 1). \tag{2.1}$$

Since $x \equiv 1 \bmod 4$, $x^2 + x + 1 \equiv 3 \bmod 4$, so $x^2 + x + 1$ is odd. Moreover, $x^2 + x + 1 = (x + 1/2)^2 + 3/4 > 0$, so $x^2 + x + 1 \geq 3$. Therefore $x^2 + x + 1$ has prime factors, and it must have a prime factor $p \equiv 3 \bmod 4$ (otherwise all its prime factors are $1 \bmod 4$, but then that means $x^2 + x + 1 \equiv 1 \bmod 4$, which is false). Since p is a factor of $x^2 + x + 1$, p divides

y^2+4 by (2.1), so $y^2+4 \equiv 0 \bmod p$. Therefore $-4 \equiv \square \bmod p$, so $-1 \equiv \square \bmod p$ since 4 is a square. But $-1 \not\equiv \square \bmod p$ when $p \equiv 3 \bmod 4$, so we have a contradiction. $\square$

Theorem 2.2. *The equation $y^2 = x^3 - 6$ has no integral solutions.*

Proof. Assume there is an integral solution. If x is even then $y^2 \equiv -6 \equiv 2 \bmod 8$, but $2 \bmod 8$ is not a square. Therefore x is odd, so y is odd and $x^3 = y^2 + 6 \equiv 7 \bmod 8$. Also $x^3 \equiv x \bmod 8$ (true for any odd x), so $x \equiv 7 \bmod 8$.

Rewrite $y^2 = x^3 - 6$ as

$$y^2 - 2 = x^3 - 8 = (x-2)(x^2+2x+4). \tag{2.2}$$

Since $x^2+2x+4 = (x+1)^2+3$ is positive, it must have a prime factor $p \equiv \pm 3 \bmod 8$ because if all of its prime factors are $\pm 1 \bmod 8$ then $x^2+2x+4 \equiv \pm 1 \bmod 8$, which is not true. Let p be a prime factor of x^2+2x+4 with $p \equiv \pm 3 \bmod 8$. Since p divides y^2-2 by (2.2), we get $y^2 \equiv 2 \bmod p$. Thus $2 \equiv \square \bmod p$, so from the conjecture about when $2 \bmod p$ is a square we get $p \equiv \pm 1 \bmod 8$, which is a contradiction because our p is $\pm 3 \bmod 8$. $\square$

Theorem 2.3. *The equation $y^2 = x^3 + 46$ has no integral solutions.*

Proof. Assume there is an integral solution. If x is even then $y^2 \equiv 46 \equiv 6 \bmod 8$, which has no solution, so x is odd and therefore y^3 is odd, so y is odd. Thus $y^2 \equiv 1 \bmod 8$ and $x^3 \equiv x \bmod 8$, so $1 \equiv x + 6 \bmod 8$, making $x \equiv 3 \bmod 8$.

Now rewrite $y^2 = x^3 + 46$ as

$$y^2 + 18 = x^3 + 64 = (x+4)(x^2-4x+16). \tag{2.3}$$

Since $x \equiv 3 \bmod 8$, the first factor on the right side of (2.3) is $7 \bmod 8$.

There is no solution to $y^2 = x^3 + 46$ when y^2 is a perfect square less than 46 (just try $y^2 = 0, 1, 4, 9, 16, 25, 36$; there is no corresponding integral x), which means we must have $x^3 > 0$, so $x > 0$. Thus $x + 4 > 1$. Since $x + 4 \equiv 7 \bmod 8$, $x + 4$ must have a prime factor p which is not 1 or $3 \bmod 8$. Indeed, if all the prime factors of $x + 4$ are 1 or $3 \bmod 8$ then so is $x + 4$, since $\{1, 3 \bmod 8\}$ is closed under multiplication. But $x + 4 \not\equiv 1, 3 \bmod 8$. The prime p, not being $3 \bmod 8$, is in particular not equal to 3. Also, $p \neq 2$ since $x + 4$ is odd. Since $p|(x+4)$ we get by (2.3) that $p|(y^2+18)$, so $y^2 \equiv -18 \bmod p$. Hence $-18 \equiv \square \bmod p$, so $-2 \equiv \square \bmod p$. This implies, from our conjecture about when $-2 \bmod p$ is a square, that $p \equiv 1$ or $3 \bmod 8$. But our p is not 1 or $3 \bmod 8$, so we have a contradiction. $\square$