Solutions to $x^2 + y^2 + 1 \equiv 0 \pmod{p}$

The USSR Olympiad Problem Book, by D. O. Shklarski, N . N. Chentzov, and I. M. Yaglom.

#248. Prove that, for any prime p, it is possible to find integers x and y such that $x^2 + y^2 + 1$ is divisible by p.

Proof. If $p = 2$, then $x = 0,\ y = 1$ is a solution, so assume p is an odd prime $(p \geq 3)$. To get the idea, consider squares in the case $p = 11$:

$0^2 \equiv 0$	$6^2 \equiv 3$
$1^2 \equiv 1$	$7^2 \equiv 5$
$2^2 \equiv 4$	$8^2 \equiv 9$
$3^2 \equiv 9$	$9^2 \equiv 4$
$4^2 \equiv 5$	$10^2 \equiv 1$
$5^2 \equiv 3$	

The values in the second column repeat the non-zero values in the first column in reverse order and this will be true for any p. To see this, let x be such that $1 \leq x \leq (p-1)/2$. Then:

$$(p-x)^2 \equiv p^2 - 2px + x^2 \equiv x^2 \pmod{p}.$$

Furthermore, the values in the first column don't repeat themselves. This too is generally the case. For suppose $x^2 = y^2 \pmod{p}$, where $1 \leq x \leq (p-1)/2$ and $1 \leq y \leq (p-1)/2$. Suppose without loss of generality that $x \leq y$. Then:

$$\begin{aligned} x^2 &\equiv y^2 \pmod{p} \\ y^2 - x^2 &\equiv 0 \pmod{p} \\ (y-x)(y+x) &\equiv 0 \pmod{p} \\ \text{ie } p &\mid (y-x)(y+x). \end{aligned}$$

$y + x$ is strictly between 2 and $p - 1$, so $p \nmid (y + x)$. Therefore $p \mid (y - x)$. But $y - x$ is strictly between 0 and $(p - 1)/2$, so it can't be a multiple of p unless it's 0, that is, unless $y = x$. Note the key fact about prime numbers used here, namely, that if a prime divides a product, then it divides one of the factors (Euclid's Lemma). This proves that the set of $\{x^2\}$ for $1 \leq x \leq (p-1)/2$ are all different.

The task is to find x and y with $x^2 = -(y^2 + 1)$, so make another chart for $p = 11$ running through the possibilities for x^2 and $-(y^2 + 1)$:

x	x^2	y	$-(y^2+1)$
0	0	0	10
1	1	1	9
2	4	2	6
3	9	3	1
4	**5**	4	**5**
5	3	5	7

Just like for x^2, all the possible values for y^2 are different, so the same is true for y^2+1 and for $-(y^2+1)$. That is, the values in the fourth column are all different. There are 6 items in the second column and 6 in the fourth column and all are between 0 and 10, so at least one of the values must be repeated. The red items show the solution $x = 1,\ y = 3$; the bold items show the solution $x = 4,\ y = 4$.

This argument can be made for any prime p: the second column has $(p+1)/2$ different values between 0 and $p-1$ and the fourth column has $(p+1)/2$ different values between 0 and $p-1$, so at least one value must appear in both columns (otherwise there would be $p+1$ values all differing from each other, impossible because they are all between 0 and $p-1$). The associated values of x and y provide a solution to $x^2+y^2+1 \equiv 0 \pmod{p}$. **QED.**

The entire argument goes through if 1 is replaced by any integer k: for any $k \in \mathbb{Z}$, there are x and y between 0 and $(p-1)/2$ such that $x^2+y^2+k \equiv 0 \pmod{p}$.

– Mike Bertrand
May 30, 2024