ELEMENTARY NUMBER THEORY

HOMEWORK 4

(1) *Show that $y^2 = x^3 + 7$ has no integer solutions.*

Hints: (This proof is due to V.A. Lebesgue)

(a) *Show that x is odd.*
If x is even, then $y^2 \equiv 7 \bmod 8$: contradiction.

(b) *Write the equation as $y^2 + 1 = x^3 + 8$ and factor the right hand side.*
$y^2 + 1 = (x + 2)(x^2 - 2x + 4)$

(c) *Show that the quadratic factor is divisible by some prime $p \equiv 3 \bmod 4$.*
Since x is odd, we have $x^2 \equiv 1 \bmod 8$ and $2x \equiv 2 \bmod 4$, hence $x^2 - 2x + 4 \equiv 3 \bmod 4$. Moreover, both factors are positive since $y^2 + 1 > 0$ and the quadratic factor has negative discriminant. Thus $x^2 - 2x + 4$ is divisible by a prime $p \equiv 3 \bmod 4$. (Note that we need the positivity: $-5 \equiv 3 \bmod 4$, but no prime $p \equiv 3 \bmod 4$ divides -5).
Here's a different solution: we claim that $x \equiv 1 \bmod 4$; in fact we have $x^3 = x \cdot x^2 \equiv x \bmod 8$ for all odd x, hence $y^2 = x^3 + 7 \equiv x + 3 \bmod 4$, and since squares cannot be $\equiv 2 \bmod 4$, the claim follows. But now $x \equiv 1 \bmod 4$ implies $x + 2 \equiv 3 \bmod 4$, hence the first factor is also divisible by a prime $p \equiv 3 \bmod 4$.

(d) *Look at the left hand side.*
We have seen that the right hand side is divisible by a prime $p \equiv 3 \bmod 4$. This implies $y^2 \equiv -1 \bmod p$, which is a contradiction since $(-1/p) = -1$ for primes $p \equiv 3 \bmod 4$.

(2) *Generalize the preceding exercise to an infinite family of diophantine equations $y^2 = x^3 + c$.*

Remark: diophantine equations of the form $y^2 = f(x)$, where $f(x)$ is a polynomial of degree 3 or 4 without multiple roots, are known as elliptic curves. During the 20th century, a vast amount of results was established for elliptic curves, and it was the theory of elliptic curves that allowed Wiles to prove Fermat's Last Theorem.

The simplest generalization is the following: put $c = 8k^3 - 1$ for some odd k. Then $y^2 = x^3 + c \equiv x^3 - 1$ implies that $x \equiv 1 \bmod 4$ as above, and the rest of the proof is the same.

In general, however, you must be very careful not to fall into one of many traps. Consider for example the case $c = m^3 - n^2$ and assume that $m \equiv 2 \bmod 4$. There cannot be a general proof that $y^2 = x^3 + c$ has no integral solution because for $m = n = 2$ we have $c = 4$ and $y^2 = x^3 + 4$ has the solutions $(0, \pm 2)$.

Assume therefore that in addition we have $n \equiv 1 \bmod 2$. Then $c \equiv -n^2 \equiv -1 \bmod 4$, hence $x \equiv 1 \bmod 4$ as above. Now $y^2 + n^2 = (x + m)(x^2 - mx + m^2)$. Since $x + m \equiv 1 + 2 \equiv 3 \bmod 4$, there is a prime

$p \equiv 3 \bmod 4$ dividing the left hand side. Now we come across the second trap: if $p \mid n$, then we will not get a contradiction because it is perfectly possible that $p \mid y$, too. In order to exclude this possibility we have to demand that n is not divisible by any prime $p \equiv 3 \bmod 4$, and then the proof actually goes through:

> Assume that $m \equiv 2 \bmod 4$ and $n \equiv 1 \bmod 2$ are integers such that n is not divisible by any prime $p \equiv 3 \bmod 4$. Then the diophantine equation $y^2 = x^3 + c$ with $c = m^3 - n^2$ does not have any integral solutions.
>
> In fact the condition on n is necessary, as the example $m = 2$, $n = 3$ shows: $y^2 = x^3 - 1$ has the integral solution $(1, 0)$ (note that our proof showed that y must be divisible by 3).

Note that even in the case where n is even we can go further; for example, there are no soltions if $m = 2M$ with $M \equiv 3 \bmod 4$ and $n = 2N$ with N odd. Are there other cases you can handle?

(3) (Euler) *Prove that if $p \equiv 1 \bmod 4$ is prime and $a = \frac{p-1}{4} - n - n^2$, then $(q/p) = +1$ for every $q \mid a$.*

We have $4a = p - (2n+1)^2$; thus every odd $q \mid a$ satisfies $p \equiv (2n+1)^2 \bmod q$, hence if $p \neq q$ we find that $(q/p) = +1$.

If $q = 2$, we have to work a little harder. In this case, $p \equiv (2n+1)^2 \bmod 4a$, hence $p \equiv (2n+1)^2 \bmod 8$ (since $2 \mid a$), and this shows that $(2/p) = 1$ by the second supplementary law.

(4) (Euler) If*$p \equiv 1 \bmod 4$ is prime, then $\frac{p-1}{4} - n(n+1)$ is a quadratic residue modulo p for every integer n.*

We have $\frac{p-1}{4} - n(n+1) \equiv \frac{p-1}{4} \bmod n$. This is a square moduo p if and only if $p - 1 - 4n(n-1) \equiv -(2n+1)^2 \bmod p$ is, and this is true for primes $p \equiv 1 \bmod 4$ (not dividing $2n+1$).