

Numbers Sheet 6

May 5, 2005

1. For which odd primes is it true that $\left(\frac{-2}{p}\right) = 1$?

We know that $\left(\frac{-1}{p}\right) = 1$ iff $p \equiv 1 \pmod{4}$ and $\left(\frac{2}{p}\right) = 1$ iff $p \equiv \pm 1 \pmod{8}$.
But $\left(\frac{-2}{p}\right) = 1$ iff $\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)$ which is true iff $p \equiv 1, 3 \pmod{8}$.

2. Determine the integers which can be written in the form $a^2 + 2b^2$ where $a, b \in \mathbb{Z}$.

We call the set of such integers S_{-2} . It is closed under product because $(a^2 + 2b^2)(c^2 + 2d^2) = N(a + b\sqrt{-2})N(c + d\sqrt{-2}) = N((a + b\sqrt{-2})(c + d\sqrt{-2}))$.

Now suppose that q is an odd prime that divides $a^2 + 2b^2$. I claim that either $q \equiv 1, 3 \pmod{8}$ or else $q|b$ and $q|a$ and so $q^2|a^2 + 2b^2$. To see these note that if $q|b$, then $q|a$ and so $q^2|a^2 + 2b^2$. If $q \nmid b$, then $(ab^{-1})^2 = -2 \pmod{q}$ and so $q \equiv 1, 3 \pmod{8}$ by the first question. Next we wish to characterise those odd primes in S_{-2} as precisely those q such that $q \equiv 1, 3 \pmod{8}$. One direction is clear from the 1st paragraph. We prove the other direction by induction on q . Let us assume that q is the smallest prime congruent to $1, 3 \pmod{8}$ which we do not know to be in S_{-2} . Since $\left(\frac{-2}{q}\right) = 1$, there exists g such that $0 < g < q/2$ and $g^2 + 2 = 0 \pmod{q}$. Thus $g^2 + 2 = qk$ where $k < q$. Choose a, b such that $a^2 + 2b^2 = ql$ where l is minimal and so $l \leq k < q$. We wish to show that $l = 1$.

First assume that l is even. Then so is a and hence $b^2 + 2(a/2)^2 = ql/2$ contradicting the minimality of l . So l must be odd.

Now assume that some odd prime p divides l . If p is not congruent to $1, 3 \pmod{8}$ then $p|b$ and $p|a$ and so $(a/q)^2 + 2(b/q)^2 = ql/p^2$ which again contradicts the minimality of l . Consequently, $p \equiv 1, 3 \pmod{8}$, $p < q$ and so by our inductive hypothesis, there exist c, d such that $c^2 + 2d^2 = p$.

Now $(a/b)^2 = -2 = (c/d)^2$ and so either $a/b = c/d \pmod{p}$ or else $a/b = -c/d \pmod{p}$. In the first case, $p|(ad - bc)$. So we consider $(a + b\sqrt{-2})/(c + d\sqrt{-2}) = (ac - 2bd)/p + \sqrt{-2}(ad - bc)/p$ whose norm is $ql/p = ((ac - 2bd)/p)^2 + 2((ad - bc)/p)^2$. Now $(ad - bc)/p$ is an integer, ql/p is an integer and so $(ac - 2bd)/p$ must also be an integer and again we have a contradiction to the minimality of l . All that remains is the case where $a/b = -c/d \pmod{p}$ in which case $p|(ad + bc)$. So we consider

$(a + b\sqrt{-2})/(c - d\sqrt{-2}) = (ac + 2bd)/p + \sqrt{-2}(ad + bc)/p$ whose norm is $ql/p = ((ac + 2bd)/p)^2 + 2((ad + bc)/p)^2$. Now $(ad + bc)/p$ is an integer, ql/p is an integer and so $(ac + 2bd)/p$ must also be an integer and again we have a contradiction to the minimality of l .

The only possibility remaining is that $l = 1$ and so $q = a^2 + 2b^2$. By induction we deduce that every odd prime congruent to $1, 3 \pmod{8}$ lies in S_{-2} .

We note that $0^2 + 2 \cdot 1^2 = 2 \in S_{-2}$ as well. Finally let $n = \prod_i p_i^{a_i}$ be the prime factorisation of n . We claim that $n \in S_{-2}$ iff $p_i = 5, 7 \pmod{8} \Rightarrow 2|a_i$. Certainly all such numbers lie in S_{-2} because S_{-2} is closed under products and contains 2, all primes congruent to $1, 3 \pmod{8}$ and all p^2 where $p = 5, 7 \pmod{8}$.

Conversely, let $n \in S_{-2}$ be the smallest element not known to be of this form. Assume that $p_i = 5, 7 \pmod{8}$; then we know that $p_i^2 | n$ and $n/p_i^2 \in S_{-2}$. It is known to be of this form by our inductive assumption and so n is also of this form.

3. Find all the solutions to $x^2 = 22 \pmod{441}$.

$441 = 9 \cdot 49$. The solutions to $x^2 = 22 \pmod{9}$ are by inspection $x = \pm 2$. The solutions to $x^2 = 22 \pmod{7}$ are $x = \pm 1$. We set $x = 1 + 7y$ and consider the equation $22 = (1 + 7y)^2 \pmod{49} = 1 + 14y \pmod{49}$ or equivalently $3 = 2y \pmod{7}$ so $y = -2 \pmod{7}$ and $x = -13 \pmod{49}$. We do not have to lift the solution $x = -1 \pmod{7}$ explicitly since the answer must be $x = 13 \pmod{49}$. The solution to the congruences $x = 2 \pmod{9}$ and $x = 13 \pmod{49}$ is $x = 209 \pmod{441}$. The solution to the congruences $x = 2 \pmod{9}$ and $x = -13 \pmod{49}$ is $x = -160 \pmod{441}$. Therefore the complete solutions to $x^2 = 22 \pmod{441}$ are $x = \pm 160, \pm 209 \pmod{441}$.