Math 445 Homework 4 Solutions

16. [NZM p.59, # 56] Suppose p is prime, and $x^2 \equiv -2 \pmod{p}$. By looking at the numbers $u + xv$ for u, v in some range, show that at least one of the equations

$$a^2 + 2b^2 = p \qquad \text{or} \qquad a^2 + 2b^2 = 2p$$

has a solution.

Following the lead of our proof for sums of squares, set $k = \lfloor \sqrt{p} \rfloor$, so

$$k = \lfloor \sqrt{p} \rfloor \le \sqrt{p} \le \lceil \sqrt{p} \rceil \le \lfloor \sqrt{p} \rfloor + 1 = k + 1 \ .$$

This implies that $k^2 \le p \le (k+1)^2$. Note that $k^2 = p$ is impossible, since p is prime. So $k^2 < p$. By the same reasoning, $(k+1)^2 = p$ is impossible, so $p < (k+1)^2$.

Now look at the collection of integers $u+xv$ for $0 \le u, v \le k$. Since there are $(k+1)^2$ possible choices of pairs (u, v), at least two of the integers $u + xv$ are congruent, mod p. So $u + xv \equiv U + xV$ for some distinct pair $(u, v) \ne (U, V)$. This implies that $u - U \equiv x(V - v)$, so, setting $a = u - U$, $b = V - v$, $a^2 \equiv x^2b^2 \equiv -2b^2 \pmod{p}$, so $a^2 + 2b^2 \equiv 0 \pmod{p}$. So $p | a^2 + 2b^2$, so $a^2 + 2b^2 = kp$ for some k. But since $0 \le u, U, v, V \le k$, $|a|, |b| \le k$ (and at least one of them is $\ne 0$, otherwise $u = U$ and $v = V$), so

$$0 < a^2 + 2b^2 \le k^2 + 2k^2 = 3k^2 < 3p \ .$$

So either $a^2 + 2b^2 = p$ or $a^2 + 2b^2 = 2p$ (since these are the only multiples of p strictly between 0 and $3p$. So at least one of the equations

$$a^2 + 2b^2 = p \qquad \text{or} \qquad a^2 + 2b^2 = 2p$$

has a solution.

17. [NZM p.60, # 57] Show that

$$(a^2 + 2b^2)(c^2 + 2d^2) = (ac - 2bd)^2 + 2(bc + ad)^2$$

$(a^2 + 2b^2)(c^2 + 2d^2) = a^2c^2 + 2a^2d^2 + 2b^2c^2 + 4b^2d^2$. On the other hand,

$(ac - 2bd)^2 + 2(bc + ad)^2$
$= ((ac)^2 - 2(ac)(2bd) + (2bd)^2) + 2((bc)^2 + 2(bc)(ad) + (ad)^2)$
$= a^2c^2 - 4abcd + 4b^2d^2 + 2b^2c^2 + 4abcd + 2a^2d^2$
$= a^2c^2 + 2a^2d^2 + 2b^2c^2 + 4b^2d^2$

So $(a^2 + 2b^2)(c^2 + 2d^2) = (ac - 2bd)^2 + 2(bc + ad)^2$, as desired.

18. [NZM p.60, # 58] Show that if p is prime and odd and $a^2 + 2b^2 = 2p$, then a is even and b is odd. Conclude that $b^2 + 2(a/2)^2 = p$ is a solution in the integers.

If $a^2 + 2b^2 = 2p$, then $a^2 + = 2p - 2b^2 = 2(p - b^2)$, so a^2 is even, so a is even . Then $a = 2c$ for some c, so $2p = (2c)^2 + 2b^2 = 2(2c^2 + b^2)$, so $p = 2c^2 + b^2$. So $b^2 = p - 2c^2$ is odd (since p is), so b is odd.

In particular, we just showed that $p = 2c^2 + b^2 = b^2 + 2(a/2)^2$, so $x^2 + 2y^2 = p$ has a solution whenever $x^2 + 2y^2 = 2p$ does (and p is odd).

19. [NZM p.60, # 59] Let p be a prime factor of the number $a^2 + 2b^2$. Show that if $p \not| a$ or $p \not| b$ then the equation $x^2 \equiv -2 \pmod{p}$ has a solution.

We have $p | a^2 + 2b^2$, so $a^2 \equiv -2b^2 \pmod{p}$. If $p \not| b$, then since p is prime, $(p, b) = 1$, so there is a y with $by \equiv 1 \pmod{p}$ (in fact, $y = b^{p-2}$ works, by FLT). Then $(ay)^2 = a^2y^2 \equiv -2b^2y^2 = -2(by)^2 \equiv -2(1) = -2 \pmod{p}$, so $x = ay$ is a solution to $x^2 \equiv -2 \pmod{p}$.

If, on the other hand, $p \not| a$; but if $b = ps$, then $a^2 + 2b^2 = a^2 + p(2ps^2) = pr$, so $a^2 = p(r - 2ps^2)$. So $p|a^2$, so $p|a$ (since p is prime), a contradiction. So $p \not| a$ implies $p \not| b$, and then the argument above applies to give a solution to $x^2 \equiv -2 \pmod{p}$.

So in either case, $x^2 \equiv -2 \pmod{p}$ has a solution.

20. [NZM p.60, # 60] Show that for any prime number p , the equation $a^2 + 2b^2 = p$ has a solution $a, b \Leftrightarrow$ the equation $x^2 \equiv -2 \pmod{p}$ has a solution x.

If $a^2 + 2b^2 = p$ has a solution, then $a \neq 0$ and $b \neq 0$, since otherwise $p = 2b^2$ or $p = a^2$ is not prime. So in particular $a^2 < p$ and $b^2 < p$, so $|a| < p$ and $|b| < p$, and so $p \not| a$ and $p \not| b$. So by Problem #19, since p is a prime factor of $p = a^2 + 2b^2$, the equation $x^2 \equiv -2 \pmod{p}$ has a solution.

On the other hand, if p is prime and $x^2 \equiv -2 \pmod{p}$ has a solution, then by Problem #16, either $a^2 + 2b^2 = p$ or $a^2 + 2b^2 = 2p$ has a solution. If p is even, then $p = 2$, and $2 = 0^2 + 2(1)^2$ so $p = a^2 + 2b^2$ has a solution. Otherwise p is odd and either Problem #16 has told us that $a^2 + 2b^2 = p$ has a solution or $a^2 + 2b^2 = 2p$ has a solution. If it is the latter, then by Problem #18 , $a^2 + 2b^2 = p$ also has a solution. So in every case, $a^2 + 2b^2 = p$ has a solution. So no matter what prime p we have, if $x^2 \equiv -2 \pmod{p}$ has a solution, then $a^2 + 2b^2 = p$ has a solution.