AC, December 2008

M3P14 Elementary Number Theory
Sheet 4: Solutions.

(1) From the way we did things in class, it is natural to take these assertions in the order (i), (iii), (iv), (ii); I am sorry if this has caused you some difficulty.
(i) We want to show that

$$\frac{n^2-1}{8} \quad \text{is} \quad \begin{cases} \text{even if} & n \equiv 1,7 \mod 8 \\ \text{odd if} & n \equiv 3,5 \mod 8 \end{cases}$$

There are four small calculations to do. For example, if $n = 8k+1$, then

$$n^2 = 64k^2 + 16k + 1$$

and $\frac{n^2-1}{8} = 2k(4k+1)$ is even. Similarly, if $n = 8k+3$, then

$$n^2 = 64k^2 + 48k + 9$$

and $\frac{n^2-1}{8} = 2k(4k+3)+1$ is odd. The cases $n = 8k+5$ and $n = 8k+7$ are similar.
(iii) Let us write $a = 2k+1$ and $b = 2h+1$. Then

$$a^2b^2 - a^2 - b^2 - 1 = (a^2-1)(b^2-1) = 16kh(k-1)(h-1)$$

is divisible by 16, therefore

$$\frac{a^2b^2 - a^2 - b^2 - 1}{8} = \frac{a^2b^2-1}{8} - \frac{a^2-1}{8} - \frac{b^2-1}{8} \equiv 0 \mod 2.$$

(iv) Follows almost immediately from (iii).
(ii) We know that if p is an odd prime then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if} \quad p \equiv 1,7 \mod 8 \\ -1 & \text{if} \quad p \equiv 3,5 \mod 8 \end{cases}$$

By what we did in part (i) then

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} \tag{1}$$

if n is prime. The result follows for all n by factorizing n into primes, because boths sides of Equation 1 are multiplicative in n.

(2) Here we go:

$$\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{2}{3}\right) = -1;$$
$$\left(\frac{13}{13}\right) = 0;$$
$$\left(\frac{456}{123}\right) = \left(\frac{-36}{123}\right) = \left(\frac{-1}{123}\right)\left(\frac{6}{123}\right)^2 = \left(\frac{-1}{123}\right)0^2 = 0;$$
$$\left(\frac{11}{10001}\right) = \left(\frac{10001}{11}\right) = \left(\frac{2}{11}\right) = -1.$$

(4)(i) Since $\mathbb{Z}/p\mathbb{Z}$ is a field, the quadratic formula holds

$$x = \frac{-b \pm \sqrt{\Delta}}{2a}$$

So one solution if $\Delta \equiv 0 \mod p$, two solutions if p does not divide Δ and Δ is a quadratic residue, and no solutions if if p does not divide Δ and Δ is a quadratic nonresidue.

(ii) I should have stated that 31957 is a prime number although it is not too much of a chore to show that it is prime; the square root is about 178 and you only have to test divisibility by primes up to 178; there are 40 primes smaller than 178, so with a pocket calculator you "only" have to perform 40 divisions.

In any case, by the first part, the equation has a solution if and only if the discriminant

$$\Delta = 9 + 4 = 13$$

is a square mod 31957. We calculate the Jacobi symbol

$$\left(\frac{31957}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1:$$

the equation does have a solution.

(5) As we know, $\mathbb{Z}/p\mathbb{Z}^\times$ is a cyclic group of order $p-1$. Property (F) says: an element $g \in \mathbb{Z}/p\mathbb{Z}^\times$ is a generator if and only if g is not a square. Wiewing the group additively: $\mathbb{Z}/p\mathbb{Z}^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$, this translates into: an element of the *additive* group $\mathbb{Z}/(p-1)\mathbb{Z}$ is a generator if and only if it is odd. In general, for all positive integers m, an element $a \in \mathbb{Z}/m\mathbb{Z}$ is an (additive) generator if and only if $\mathrm{hcf}(a, m) = 1$. We can finally re-phrase property (F) as follows:

Property (F) for a prime p: $\mathrm{hcf}(a, p-1) = 1$ if and only if a is odd.

From here, it is easy to see that a prime p satisfies property (F) if and only if it is of the form 2^{2^n}.

(6) (i) This always happense if $\mathrm{hcf}(a, n) = 1$ and a is a square mod n. Indeed then a is a square mod p for every prime p that divides n, so $\left(\frac{a}{p}\right) = 1$ for every prime that divides n, and then $\left(\frac{a}{n}\right) = 1$ by definition of the Jacobi symbol.
(ii) This can happen if $\mathrm{hcf}(a, n) \neq 1$; for example if $n = p$ is prime, and $p|a$, then by definition $\left(\frac{a}{p}\right) = 0$ but $a \equiv 0 \mod p$ is certainly a square mod p.
(iii) This can happen and we saw an example in class; take $n = 15$ and $a = -1$; then $\left(\frac{-1}{15}\right) = 1$ but -1 is not a square mod 15.
(iv) This can also happen; for example every time that $n = p$ is prime and $p \not| a$.

(8) This is fun: first, we look at

$$y^2 = x^3 + 23$$

modulo 4; $y^2 \equiv 0$ or $1 \mod 4$; correspondingly, $x^3 \equiv 1$ or $2 \mod 4$; but only the first case is possible with $x \equiv 1 \mod 4$ and y even.

Now we have

$$y^2 + 4 = x^3 + 27 = (x+3)(x^2 - 3x + 9)$$

and the factor $x^2 - 3x + 9 \equiv 3 \mod 4$, so it is the product of odd primes and at least one of them, say $p \equiv 3 \bmod 4$. From

$$y^2 + 4 \equiv 0 \mod p$$

we get $\left(\frac{-1}{p}\right) = 1$, a contradiction.

(10) This problem tests your understanding of the method of Fermat descent. Whether you guessed correctly or not, the answer is: If p is an odd prime, then the equation

$$x^2 + 2y^2 = p$$

is soluble for integers x, y if and only if $p \equiv 1$ or $3 \mod 8$.

Indeed, if a solution exists then -2 is a residue mod p, that is

$$\left(\frac{-2}{p}\right) = 1$$

and the condition follows from our knowledge of the Legendre symbol.

Viceversa, let us assume that $\left(\frac{-2}{p}\right) = 1$. First, we can find integers A, B and $0 < M < p$ such that

$$A^2 + 2B^2 = Mp$$

Indeed, by choosing $-p/2 < A, B < p/2$ (and coprime with p) such that $A^2 + 2B^2 \equiv 0 \mod p$, we also ensure that

$$A^2 + 2B^2 = Mp < \frac{1}{4}p^2 + 2 \times \frac{1}{4}p^2 = \frac{3}{4}p^2, \quad \text{hence} \quad M < p.$$

Now if $M = 1$ we are done, so let us assume that $M > 1$. We try to set up a machine to make M smaller.

Everything is based on the *key identity*:

$$(A^2 + 2B^2)(u^2 + 2v^2) = (Au + 2Bv)^2 + 2(Bu - Av)^2$$

(Verify the identity, play with it, make sure you understand it.)

Choose u, v with

$$\begin{cases} u \equiv A \mod M \\ v \equiv B \mod M \end{cases} \quad \text{and} \quad -\frac{M}{2} \leq u, v < \frac{M}{2}.$$

we get that $u^2 + 2v^2 \equiv A^2 + 2B^2 \equiv 0 \mod M$, hence we can write

$$u^2 + 2v^2 = rM$$

for some integer $0 < r$, and note that, since:

$$u^2 + 2v^2 \leq \frac{1}{4}M^2 + 2 \times \frac{1}{4}M^2 < M^2,$$

we also get that $r < M$. But now by the key identity:

$$(A^2 + 2B^2)(u^2 + 2v^2) = (Au + 2Bv)^2 + 2(Bu - Av)^2 = rM^2p$$

and $Au+2Bv \equiv u^2+2v^2 \equiv 0 \mod M$, and $Bu-2Av \equiv BA-AB \equiv 0 \mod M$, so, dividing through by M:

$$\Big(\frac{Au+2Bv}{M}\Big)^2 + \Big(\frac{Bu-Av}{M}\Big)^2 = rp$$

and, as I said before, $0 < r < M$. We are done be descending induction (or 'descent', à la Fermat).

As a final note: You could have done all of this by studying the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-2})$, with ring of integers $\mathcal{O} = \mathbb{Z}[i\sqrt{2}]$: show that $\mathcal{O}$ is a Euclidean domain (with the logical norm), study the *primes* in $\mathcal{O}$, etcetera.

(12)(i) This could be interpreted as a routine exercise on the Euclidean algorithm in $\mathbb{Z}[i]$. It is more fun to do it thus:

(a) Let us first compute norms: $8+38i = 2(4+19i)$ and $N(4+19i) = 16+361 = 377 = 13 \times 29$. Now $13 = 9+4 = (3+2i)(3-2i)$ is the prime decomposition in $\mathbb{Z}[i]$ and it follows that either $3+2i|4+19i$ or $3-2i|4+19i$. A small experiment shows that the latter holds:

$$8+38i = 2(4+19i) = -i(1+i)^2(3-2i)(-2+5i)$$

and this *must* be the prime decomposition of $8+38i$ in $\mathbb{Z}[i]$ (why?)—note that these are not *normalised* primes, but who cares.

Similarly, $N(9+59i) = 81+3841 = 3562 = 2\times 13\times 137$. A small experiment shows that

$$9+59i = (3-2i)(-7+15i)$$

(is this the prime decomposition of $9+59i$ in $\mathbb{Z}[i]$?). From this we can conclude that

$$\mathrm{hcf}(8+38i, 9+59i) = (1+i)(3-2i)$$

(supply your own argument based on this or finish computing the prime factorisation of $9+59i$ in $\mathbb{Z}[i]$ and conclude from there...).

(b) From part (a) we know all about $-19+4i$:

$$-19+4i = i(4+19i) = i(3-2i)(-2+5i)$$

–the prime decomposition in $\mathbb{Z}[i]$. Now $N(-9+19i) = 81+361 = 442 = 2\times 13\times 17$; we check if $-9+19i$ is divisible by $3-2i$:

$$\frac{-9+19i}{3-2i} = \frac{(-9+19i)(3+2i)}{13} = \frac{-65+39i}{13} = -5+3i.$$

It is, so we conclude $\mathrm{hcf}(-19+4i, -9+19i) = 3-2i$.

(ii) The answer is—remember: we want *normalised* primes:

$$23-11i = -(1+i)(2+i)^2(2+3i)$$

The first thing you should have done is to calculate the norm:

$$23^2+11^2 = 650 = 2\times 25\times 13$$

From this it is clear that $(1+i)$, for example, divides $\alpha = 23-11i$ (why?); also either $(2+i)^2$ or $(2-i)^2$ divides α, but not both (why?); and $3+2i$ or $3-2i$ divides α (but not both). You can then find what exactly is going on by trial and error. Finally you have to be a bit careful: for instance, $3-2i$ divides α but it is not normalized: you have to use $i(3-2i)=2+3i$ instead!

(14) $2925 = 3^2 \times 5^2 \times 13$; the divisors $d \equiv 1 \mod 4$ are

$$1, 5, 9, 13, 25, 45, 65, 117, 225, 325, 585, 2925$$

and those $\equiv 3 \mod 4$ are

$$3, 15, 39, 75, 195, 975.$$

Hence $D_1 = 12$, $D_3 = 6$ and there are 24 integer pairs of solutions of the equation

$$x^2 + y^2 = 2925$$

Explicitly to enumerate the solutions, it is best to go back to the proof. The prime factorisation of $n = 2925$ in $\mathbb{Z}[i]$ is:

$$2925 = (2+i)^2(2-i)^2(3+2i)(3-2i) \times 3^2$$

Solutions of $x^2 + y^2 = 2925$ are given by

$$\begin{aligned}
x + iy &= u(2+i)^2(3+2i) = u(1+18i);\\
&= u(2+i)^2(3-2i) = u(17+6i);\\
&= u(2+i)(2-i)(3+2i) = u(15+10i);\\
&= u(2+i)(2-i)(3-2i) = u(15-10i);\\
&= u(2-i)^2(3+2i) = u(17-6i);\\
&= u(2-i)^2(3-2i) = u(1-18i).
\end{aligned}$$

where u can be any unit: ± 1 or $\pm i$ (for a total of $6 \times 4 = 24$ solutions). The 24 solutions are: $(\pm 1, \pm 18)$, $(\pm 18, \pm 1)$ (8 solutions); $(\pm 6, \pm 17)$, $(\pm 17, \pm 6)$ (8 solutions); and $(\pm 10, \pm 15)$, $(\pm 15, \pm 10)$ (8 solutions).