189-346/377B: Number Theory
Solutions to Assignment 6

1. Let p be an odd prime. Show that -2 is a quadratic residue modulo a prime p if and only if p is a prime of the form $m^2 + 2n^2$.

Solution: If p is of the form m^2+2n^2, then the residue class of (m/n) modulo p (which makes sense because n is non-zero modulo p!) is a square root of -2 modulo p. The interesting direction is the converse. For this, following the approach developped in class for sums of two squares, we begin by showing that the ring $\mathbf{Z}[\sqrt{-2}]$ admits unique factorisation into irreducible elements, and that in particular the gcd of two elements a and b in $\mathbf{Z}[\sqrt{-2}]$ is always a linear combination (with coefficients in $\mathbf{Z}[\sqrt{-2}]$) of a and b. To prove this, one proceeds as was done in class to show that there is a euclidean division algorithm. More precisely, given a and b in $\mathbf{Z}[\sqrt{-2}]$ with $b \neq 0$, we show that there exists q and r in that same ring such that

$$a = bq + r, \qquad r\bar{r} < b\bar{b}.$$

To see this, write $a/b = u + v\sqrt{-2}$ with $u, v \in \mathbf{Q}$, and let $q = x + y\sqrt{-2}$ be the element of $\mathbf{Z}[\sqrt{-2}$ for which the coordinates x and y are the closest integers to u and v respectively. By construction,

$$\mathrm{norm}(a/b - q) \leq (1/2)^2 + 2 \cdot (1/2)^2 = 3/4,$$

and hence

$$\mathrm{norm}(a - bq) \leq 3/4\mathrm{norm}(b).$$

Since $r = a - bq$, this concludes the claim about the Euclidean division. Now, by proceeding exactly as was done in class for $\mathbf{Z}[i]$, one shows that the *gcd* of a and b is of the form $ra + sb$ for some $r, s \in \mathbf{Z}[\sqrt{-2}]$.

Once this preparatory work is done, we reason exactly as was done in class for sums of two squares. More precisely, if -2 is a quadratic residue modulo p, then we may find an integer $t \leq (p+1)/2$ such that $t^2 + 2 =: mp$ is divisible by p, but not by p^2. Now let $a = \gcd(t + \sqrt{-2}, p)$. CLearly the

integer $a\bar{a}$ divides p, since it divides both $mp = t^2 + 2$ and p^2. But we also know that a is a linear combination of $t + \sqrt{-2}$ and p, hence its norm is congruent, modulo p, to the norm of $t + \sqrt{-2}$, which is 0 mod p, therefore the norm of a is divisible by–hence equal to–p. But writing $a = r + s\sqrt{-2}$, this gives $r^2 + 2s^2 = p$, as was to be shown.

2. Use question 1 and quadratic reciprocity to get a complete characterisation of all the integers that are of the form $m^2 + 2n^2$.

Quadratic reciprocity tells us that -2 is a quadratic residue modulo a prime p if and only if $p = 1$ or 3 modulo 8. Hence the set of *primes* of the form $m^2 + 2n^2$ is precisely the set of primes which are congruent to 1 or 3 modulo 8.

To caracterise the integers that can be written in this way, we first observe that if r is any integer of the form $m^2 + 2n^2$, then, after factoring out the common divisor d of m and n we have

$$r = d^2(m_0^2 + 2n_0^2) = d^2 r_0, \qquad \text{with } \gcd(m_0, n_0) = 1.$$

To characterize r_0, we note that any rational prime p dividing r_0 is necessarily congruent to 1, 2 or 3 modulo 8, since the class of (m_0/n_0) modulo p is a square root of -2 modulo p. It follows that any integer of the form $m^2 + 2n^2$ is necessarily of the form $d^2 p_1 \cdots p_r$, where the p_j's are primes which are congruent to 1, 2 or 3 modulo 8. Conversely, any integer of that form can certainly be written in the form $m^2 + 2n^2$–this follows from the case of primes, by the multiplicativity of the norm in $\mathbf{Z}[\sqrt{-2}]$.

3. Repeat questions 1 and 2 with $m^2 + 2n^2$ replaced by $m^2 + 3n^2$.

Solution. The ideas here are exactly the same as for the case $m^2 + 2n^2$, replacing the ring $\mathbf{Z}[\sqrt{-2}]$ by the ring $\mathbf{Z}[\sqrt{-3}]$. The final answer is that an integer r can be written in the form $m^2 + 3n^2$ is and only if it is of the form $d^2 p_1 \cdots p_r$, where d is an arbitrary integer and the p_j are primes which are either 0 or 1 modulo 3.

4. Show that there are primes p for which -5 is a quadratic residue modulo

p, yet which are not of the form $m^2 + 5n^2$.

Solution: It is not hard to produce such examples. For example, $-5 = 3^2 \pmod 7$, but 7 is not of the form $m^2 + 5m^2$, clearly. The same if true of 3 since $-5 = 1^2 \pmod 3$.

5. Make a list of the integers ≤ 100 that can be written in the form m^2+5n^2, and $2m^2+2mn+3n^2$. Can you formulate some conjectures about how these sets of integers behave? (You may find it useful to write each integer in factored form.)

Solution: The table of all integers ≤ 100 of the form m^2+5m^2 with $\gcd(m, n) = 1$, along with their factorisations, is as follows:

$$1, \quad 6 = 2 \times 3, \quad 9 = 3 \times 3, \quad 14 = 2 \times 7, \quad 21 = 3 \times 7, \quad 29 = 29,$$

$$30 = 5 \times 2 \times 3, \quad 41 = 41, \quad 45 = 3 \times 3 \times 5, \quad 46 = 2 \times 23, \quad 49 = 7 \times 7,$$

$$61 = 61, \quad 69 = 3 \times 23, 70 = 2 \times 5 \times 7, \quad 81 = 3^4,$$

$$89 = 89, \quad 94 = 2 \times 47$$

Right off the bat, there are several interesting patterns that can be inferred from this table. For instance, it appears that the primes of the form m^2+5m^2 are either equal to 5, or are congruent to 1 or 9 modulo 20. (These are the primes 29, 41, 61, and 89.) Furthermore, the same statement seems to be true of the integers that are not divisible by 2 or 5, and appear in this table. These are the integers 1, 9, 21, 29, 41, 49, 61, 69, 81 and 89. The data suggests that these are precisely the integers that are congruent to 1 or 9 modulo 20!

When examining the factorisations, one sees appearing the primes 2, 3, 7, 23 and 47, which are not of the form $n^2 + 5m^2$ even though they divide an integer of this form. On the other hand, these primes are all of the form $2m^+2mn + 3n^2$, and they are all congruent to either 3 or 7 modulo 21. From these simple observations, it would appear that, as far as the integers r that are relatively prime to 2 and 5 are concerned, they are of the form $m^2 + 5m^2$ (resp. $2m^2 + 2mn + 3n^2$) if and only if they are congruent to 1 or 9 (resp. to 3 or 7) modulo 21. Note that, in particular, of p and q are both of the form $m^2 + 5n^2$ then so is their product, while if p and q are

of the form $2m^2 + 2mn + 3n^2$, then their product is of the form $m^2 + 5m^2$. Can you explain this empirical pattern algebraically, by writing down explicit formulas for passing from a representation of p and q as a value of one of those two quadratic forms, to the desired representation for the product?

These are some of the most striking patterns you could observe... of course the question was somewhat open-ended and there was no clear "right answer"– the main point was to get you staring at these patterns and thinking about them a bit – understanding what goes on leads to the theory of Gaussian composition of binary quadratic forms and the "class group" of quadratic rings, one of the central achievements of Gauss's Disquisitiones which is nicely explained in somewhat more modern language in Granville's notes.

6. By elementary arguments (working in $\mathbf{Z}$) show that the diophantine equation $x^2 + 1 = y^n$ has no solution when

1. x is odd and $n > 1$.

2. n is even.

Use this to show that if $n > 1$, then there exists a Gaussian integer $a + bi$ for which $x + i = (a + bi)^n$. Conclude that $b = \pm 1$ and that the equation in question has no solution for $n = 3$, 5 and 7.

Solution. The first part can be done by elementary arguments. Namely, if x is odd then $x^2 + 1 \equiv 2 \pmod 4$ and hence cannot be a perfect nth power for any $n > 1$ (since the power of 2 dividing it is exactly 2). Also, if $n = 2m$ is even then the equation can be written as $(y^m - x)(y^m + x) = 1$, from which we obtain either $y^m - x = y^m + x = 1$ or $y^m - x = y^m + x = -1$, which leads (by solving linear equations!) to $y = \pm 1$ and $x = 0$. (So the second part was not quite right: there are two "trivial" solutions $(x, y) = (0, \pm 1)$ when n is even!...)

Thanks to these elementary considerations, in studying the equation $x^2 + 1 = y^n$, we may restrict our attention to the case where x is even and n is odd.

Now, for the second part of the question, we can rewrite the equation $x^2 + 1 = y^n$ as

$$(x + i)(x - i) = y^n. \tag{1}$$

But the gcd of $x+i$ and $x-i$ clearly divides $2i = (1+i)^2$, and therefore must be 1 since the fact that x is even precludes the possibility that $1+i$ divides $x+i$. By the unique factorisation principle that was explained in class, it follows that both $x+i$ and $x-i$ are perfect n-th powers in $\mathbf{Z}[i]$, up to multiplication by a unit. But since we are assuming n is odd, each of these units – namely $1, -1, i$ and $-i$– is a perfect nth power as well, and therefore there is a Gaussian integer $a+bi$ such that

$$x + i = (a+bi)^n. \tag{2}$$

Expanding the right hand side using the binomial theorem, and examining the imaginary part, we see that this imaginary part is divisible by the integer b, and therefore b divides 1, and hence $b = \pm 1$.

Now, in the case $n = 3$, the equation (2) becomes

$$x = a^3 - 3ab^2, \qquad 3a^2b - b^3 = 1.$$

From this and the fact that $b = \pm 1$, we find that $3a^2 - b^2 = \pm 1$, and therefore $3a^2 = 0$ or 2. Hence $a = 0$, so that $x = 0$, which leads to the "trivial" solution $x = 0$, $y = 1$ of the original equation. (This solution is there, so the question was not formulated correctly; but nonetheless we have shown that there are *no other* solutions aside from these obvious and not-so-interesting ones.)

7. Solve the Pell equation $x^2 - 133y^2 = 1$ by using the continued fraction method (clearly indicate all the steps that you follow).

I hope that you did this one by hand, because, although it is a bit long, it is also rather fun and it is good to gain some proficiency in calculations like this. We note first that $\sqrt{133} = 11.53....$

The following sequence of calculations:

$$\begin{aligned}
\sqrt{133} &= 11 + (\sqrt{133} - 11); \\
\frac{1}{\sqrt{133}-11} &= \frac{\sqrt{133}+11}{12} = 1 + \frac{\sqrt{133}-1}{12}; \\
\frac{12}{\sqrt{133}-1} &= \frac{12(\sqrt{133}+1)}{132} = \frac{\sqrt{133}+1}{11} = 1 + \frac{\sqrt{133}-10}{11}; \\
\frac{11}{\sqrt{133}-10} &= \frac{11(\sqrt{133}+10)}{33} = \frac{\sqrt{133}+10}{3} = 7 + \frac{\sqrt{133}-11}{3};
\end{aligned}$$

$$
\begin{aligned}
\frac{3}{\sqrt{133}-11} &= \frac{3(\sqrt{133}+11)}{12} = \frac{\sqrt{133}+11}{4} = 5+\frac{\sqrt{133}-9}{4};\\
\frac{4}{\sqrt{133}-9} &= \frac{4(\sqrt{133}+9)}{52} = \frac{\sqrt{133}+9}{13} = 1+\frac{\sqrt{133}-4}{13};\\
\frac{13}{\sqrt{133}-4} &= \frac{13(\sqrt{133}+4)}{117} = \frac{\sqrt{133}+4}{9} = 1+\frac{\sqrt{133}-5}{9};\\
\frac{9}{\sqrt{133}-5} &= \frac{9(\sqrt{133}+5)}{108} = \frac{\sqrt{133}+5}{12} = 1+\frac{\sqrt{133}-7}{12};\\
\frac{12}{\sqrt{133}-7} &= \frac{12(\sqrt{133}+7)}{84} = \frac{\sqrt{133}+7}{7} = 2+\frac{\sqrt{133}-7}{7};\\
\frac{7}{\sqrt{133}-7} &= \frac{7(\sqrt{133}+7)}{84} = \frac{\sqrt{133}+7}{12} = 1+\frac{\sqrt{133}-5}{12};\\
\frac{12}{\sqrt{133}-5} &= \frac{12(\sqrt{133}+5)}{108} = \frac{\sqrt{133}+5}{9} = 1+\frac{\sqrt{133}-4}{9};\\
\frac{9}{\sqrt{133}-4} &= \frac{9(\sqrt{133}+4)}{117} = \frac{\sqrt{133}+4}{13} = 1+\frac{\sqrt{133}-9}{13};\\
\frac{13}{\sqrt{133}-9} &= \frac{13(\sqrt{133}+9)}{52} = \frac{\sqrt{133}+9}{4} = 5+\frac{\sqrt{133}-11}{4};\\
\frac{4}{\sqrt{133}-11} &= \frac{4(\sqrt{133}+11)}{12} = \frac{\sqrt{133}+11}{3} = 7+\frac{\sqrt{133}-10}{3};\\
\frac{3}{\sqrt{133}-10} &= \frac{3(\sqrt{133}+10)}{33} = \frac{\sqrt{133}+10}{11} = 1+\frac{\sqrt{133}-1}{11};\\
\frac{11}{\sqrt{133}-1} &= \frac{11(\sqrt{133}+1)}{132} = \frac{\sqrt{133}+1}{12} = 1+\frac{\sqrt{133}-11}{12};\\
\frac{12}{\sqrt{133}-11} &= \frac{12(\sqrt{133}+11)}{12} = \sqrt{133}+11 = 22+(\sqrt{133}-11)
\end{aligned}
$$

shows that the continued fraction expansion of $\sqrt{133}$ is given by

$$\sqrt{133} = [11, \overline{1, 1, 7, 5, 1, 1, 1, 2, 1, 1, 1, 5, 7, 1, 1, 22}]$$

where the bar denotes an infinite period sequence (with period length 16). Now, the sequence of convergents is calculated in the following table:

a_n	11	1	1	7	5	1	1	1	2	1	1
p_n	11	12	23	173	888	1061	1949	3010	7969	10979	18948
q_n	1	1	2	15	77	92	169	261	691	952	1643
$p_n^2 - 133q_n^2$	-12	11	-5	4	-13	9	-12	7	-12	9	-13

a_n	1	5	7	1	1	22
p_n	29927	168583	1210008	1378591	2588599	
q_n	2595	14618	104921	119539	224460	
$p_n^2 - 133q_n^2$	4	-3	11	-12	1	

This calculation shows that the fundamental solution to $x^2 - 113y^2 = 1$ is given by $(x, y) = (2588599, 224460)$. While not exactly for the faint of heart, it is striking that such calculations can be performed *at all* without calculator or computer. Mathematicians like Fermat revelled in carrying them out in even more complicated cases— this was how he knew that the fundamental solution to the Pell equation $x^2 - 61y^2 = 1$ is $(1766319049, 226153980)$... Try doing this one if you are feeling brave!

Math 377 students only:

8. Section 8.4, Problem 4 in Leveque.

9. Section 8.4, Problem 5 in Leveque.