

MATH 4400
HOMEWORK 5
DUE 2/28/08

Instructions: Math 6400 students should do all the problems. Math 4400 students should do five of the seven problems.

Problem 1: A prime p is called a *Sophie Germain prime* if $2p + 1$ is also prime. In this case, $2p + 1$ is sometimes called the *safe prime*. Show that if $p > 3$ is a Sophie Germain prime congruent to $3 \pmod{4}$, then $2^p - 1$ is composite. (Hint: What is $2^p \pmod{2p + 1}$?)

Solution: Let $q = 2p + 1$. Notice that $\left(\frac{2}{q}\right) = 1$ because $q \equiv 7 \pmod{8}$. So $2^{(q-1)/2} \equiv 1 \pmod{q}$. But $(q-1)/2 = p$, so we get $2^p \equiv 1 \pmod{q}$, hence $q | (2^p - 1)$. For $p > 3$, it's easy to see that q is strictly smaller than $2^p - 1$, so $2^p - 1$ is composite. \square

Remark: It is not known whether or not there are infinitely many Sophie Germain primes, let alone infinitely many congruent to $3 \pmod{4}$. It is also not known whether or not there are infinitely many primes p such that $2^p - 1$ is composite.

Problem 2: Let p be an odd prime. This exercise outlines a proof that $\mathbb{Q}(\zeta_p)$ contains $\mathbb{Q}(\sqrt{p^*})$, where $p^* = \left(\frac{-1}{p}\right)p$. For the rest of the problem, let $f_p(x) = x^p - 1$ and let $\zeta = \zeta_p$.

(a) Fix i such that $0 \leq i \leq p - 1$. Show that

$$f'_p(\zeta^i) = \prod_{j \neq i} (\zeta^i - \zeta^j).$$

(Here j runs over $\{0, \dots, p - 1\}$ but skips i .)

(b) By part (a), we get

$$\prod_{i=0}^{p-1} f'_p(\zeta^i) = \prod_{i=0}^{p-1} \prod_{j \neq i} (\zeta^i - \zeta^j).$$

Show that the left side equals p^p .

(c) Now show that the right side equals

$$\left(\frac{-1}{p}\right) \prod_{i < j} (\zeta^i - \zeta^j)^2$$

where the product runs over all ordered pairs (i, j) with $0 \leq i < j \leq p - 1$. (Hint: how many terms of the right side of part (b) have to get flipped?)

(d) Conclude that $\sqrt{p^*} \in \mathbb{Q}(\zeta_p)$.

Solution: (a) This is clear, since $f'_p(x)$ is a sum of p different terms, each of which is a product of $p - 1$ linear polynomials (Product Rule!) All but one of these terms has an $(x - \zeta^i)$ factor in it, so when evaluated at ζ^i it gives 0. The remaining one is

$$\prod_{j \neq i} (x - \zeta^j),$$

so when we plug in ζ^i for x we get what we want.

(b) Well, $f'_p(\zeta^i) = p(\zeta^i)^{p-1}$, so the product of this over all i is

$$p^p \prod_{i=0}^{p-1} \zeta^{i(p-1)} = p^p \zeta^{(p-1)p(p-1)/2} = p^p$$

because $(p-1)^2/2$ is an integer.

(c) For every i and j with $i < j$, the term $(\zeta^i - \zeta^j)$ appears once on the right side of (b), and so does the term $(\zeta^j - \zeta^i)$. To convert this product into the product of $(\zeta^i - \zeta^j)^2$, we have to introduce one negative sign. Thus we have to introduce as many negative signs as there are pairs i, j with $i < j$. Of course there are $p(p-1)/2$ such pairs. So this introduces a factor of $(-1)^{p(p-1)/2} = (-1)^{(p-1)/2} = \left(\frac{-1}{p}\right)$, and we are done.

(d) Bringing the $\left(\frac{-1}{p}\right)$ to the left side of (c) and taking square roots, we get

$$\begin{aligned} \sqrt{\left(\frac{-1}{p}\right) p^p} &= \pm \prod_{i < j} (\zeta^i - \zeta^j) \\ \sqrt{p^*} &= \frac{\pm 1}{p^{(p-1)/2}} \prod_{i < j} (\zeta^i - \zeta^j) \end{aligned}$$

and the right side of this equation is in $\mathbb{Q}(\zeta)$, so we are done. \square

Problem 3: Let n be an odd positive integer. Show that

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

Solution: This runs similarly to the proofs we've done in class. Induct on the number of prime divisors of n . The base case is part of our proof of Quadratic Reciprocity. So now suppose $n = ap$, p prime, and we have proved the theorem for a (and of course for p). Then

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

so now we must show that

$$\frac{a^2-1}{8} + \frac{p^2-1}{8} \equiv \frac{(ap)^2-1}{8} \pmod{2}.$$

To see this, consider that

$$\frac{(ap)^2-1}{8} - \left(\frac{a^2-1}{8} + \frac{p^2-1}{8}\right) = \frac{(a^2-1)(p^2-1)}{8},$$

which is always even because both a^2-1 and p^2-1 are divisible by 4 (as a and p are both odd). This finishes the proof. \square

Problem 4: Show that

$$\sum_{n \leq x} \sigma_0(n) = x \ln x + O(x).$$

Solution: We have

$$\sum_{n \leq x} \sigma_0(n) = \sum_{n \leq x} \sum_{d|n} 1 = \sum_{d \leq x} 1 = \sum_{d \leq x} \sum_{e \leq x/d} 1 = \sum_{d \leq x} \left(\frac{x}{d} + O(1) \right) = \left(x \sum_{d \leq x} \frac{1}{d} \right) + O(x),$$

and since we have seen that $\sum_{d \leq x} \frac{1}{d} = O(\ln x)$, the result follows. \square

Problem 5: (a) Show that $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$ are PIDs.

(b) Show that $\mathbb{Z}[\sqrt{-3}]$ and $\mathbb{Z}[\sqrt{5}]$ are not PIDs.

Solution: (a) Consider what a division algorithm in $\mathbb{Z}[\sqrt{d}]$ would look like, for $d = 2$ or 3 . For any $a, b \in \mathbb{Z}[\sqrt{d}]$, our task would be to find $q, r \in \mathbb{Z}[\sqrt{d}]$ such that $a = bq + r$ and $|N(r)| < |N(b)|$. Here $N(x + y\sqrt{d}) = x^2 - dy^2$. Note that norms can be negative if $d > 0$, so we need to take absolute values! At any rate, this means that we can find $r = a - bq$ satisfying $|N(r/b)| < 1$. And $|N(r/b)| = |N(a/b - q)|$, so the task is to pick q close enough to a/b to make its norm sufficiently small.

So we must show, for $d = 2$ or 3 , that for any $\alpha \in \mathbb{Q}[\sqrt{d}]$ there is a $q \in \mathbb{Z}[\sqrt{d}]$ such that $\alpha - q$ has norm strictly less than 1.

For $d = 2$ this is straightforward: let $\alpha = \alpha_1 + \alpha_2\sqrt{2}$; then we can find integers q_1, q_2 such that $|\alpha_i - q_i| \leq 1/2$, so $(\alpha_i - q_i)^2 \leq 1/4$. Then

$$|N(\alpha - q)| = |(\alpha_1 - q_1)^2 - 2(\alpha_2 - q_2)^2| \leq 1/4 + 2(1/4) = 3/4,$$

and we are all set.

For $d = 3$ the same inequalities yield $|N(\alpha - q)| \leq 1$. This is all right unless equality holds. What are we to do in that case? Well, in that case there are four equally reasonable choices for q , each satisfying $\alpha - q = \pm 1/2 \pm 1/2\sqrt{3}$ (the \pm signs are independent). So pick the q satisfying $\alpha - q = 1/2 + 1/2\sqrt{3}$; then $N(\alpha - q) = 1/2 - 3(1/2)^2 = -1/2$, whose absolute value is again strictly smaller than 1.

(b) First we show that the ideal $(2, 1 + \sqrt{-3})$ is not principal in $\mathbb{Z}[\sqrt{-3}]$. First of all, it's clear that these two elements are irreducible in $\mathbb{Z}[\sqrt{-3}]$; they both have norm 4, and there is no element in $\mathbb{Z}[\sqrt{-3}]$ of norm 2. Since 2 clearly doesn't divide $1 + \sqrt{-3}$, they cannot be unit multiples of each other. So if this ideal were principal, its generator couldn't have norm 4, as then the fact that it divided 2 would imply that it was a unit multiple of 2 (take norms), and similarly it would be a unit multiple of $1 + \sqrt{-3}$, which is impossible.

But the norm of a generator of this ideal has to divide 4, because the generator has to divide 2. But there is no element of norm 2. So the only other case to rule out is that the ideal is generated by an element of norm 1, i.e. the ideal is the whole ring. Why is this not the case?

Well, suppose $1 = 2\alpha + (1 + \sqrt{-3})\beta$ for some $\alpha, \beta \in \mathbb{Z}[\sqrt{-3}]$. Then take norms of both sides. We get

$$1 = (2\alpha + (1 + \sqrt{-3})\beta)(2\bar{\alpha} + (1 - \sqrt{-3})\bar{\beta}) = 4N(\alpha) + 2(\dots) + 4N(\beta),$$

where the stuff in the parentheses is in $\mathbb{Z}[\sqrt{-3}]$. But this is impossible because the right side is divisible by 2 in $\mathbb{Z}[\sqrt{-3}]$. So that does it.

The proof for $\mathbb{Z}[\sqrt{5}]$ is similar, with the ideal $(2, 1 + \sqrt{5})$. (There are no elements of order ± 2 in $\mathbb{Z}[\sqrt{5}]$.) \square

Problem 6: (a) Find, with proof, a description of all primes p that can be written as $x^2 - 2y^2$, where $x, y \in \mathbb{Z}$.

(b) Do the same for $x^2 - 3y^2$. (Warning for both problems: careful when you run the standard argument, as norms of elements of $\mathbb{Z}[\sqrt{d}]$ might be negative!)

Solution: (a) The same argument that we used to prove Problem 7 on the previous problem set tells us that, for an odd prime p , $p = x^2 - 2y^2 \Rightarrow 2$ is a square mod $p \Rightarrow p$ is not irreducible in $\mathbb{Z}[\sqrt{2}]$. Let's see how we might try to show that they are equivalent, though: when we try to prove that the third statement implies the first, we see that, writing $p = \alpha\beta$, we get $p^2 = N(\alpha)N(\beta)$. So if α and β are nontrivial, then their norms are $\pm p$. Aha! But we can multiply α by $1 + \sqrt{2}$, if necessary, to ensure that its norm is p . So those three statements are equivalent, as usual, and we get that $p \equiv \pm 1 \pmod{8}$ (or $p = 2$).

(b) Here we have a serious problem: there is no element of $\mathbb{Z}[\sqrt{-3}]$ of norm -1 that we can use like we did in the previous argument. In fact, we cannot solve $x^2 - 3y^2 = a$ if $a \equiv -1 \pmod{3}$. So that actually helps us: the equation $p = x^2 - 3y^2$ can only have a solution if $p \equiv 1 \pmod{3}$, and in this case we can run the same argument as above, and this time we note that $-p$ cannot be the norm of something in $\mathbb{Z}[\sqrt{-3}]$, so the norms of α and β both have to be p . The conclusion is that $p = x^2 - 3y^2$ has a solution if and only if $p \equiv 1 \pmod{3}$ and 3 is a square mod p , so by quadratic reciprocity we get that $p \equiv 1 \pmod{12}$.

Problem 7: For any nonconstant polynomial $f(x) \in \mathbb{Z}[x]$, show that there are infinitely many primes p such that $f(x)$ has a root in \mathbb{F}_p .

Remark: We used this argument in the special case $f = \Phi_n$ to show that there were infinitely many primes congruent to $1 \pmod{n}$.

Solution: Suppose there were only finitely many such primes p_1, \dots, p_ℓ . Then for all $n \in \mathbb{Z}$ we have that $f(n)$ is only divisible by p_1, \dots, p_ℓ . Let $f(0) = \pm p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$. Let $m_k = f(kp_1^{\alpha_1+1} \cdots p_\ell^{\alpha_\ell+1})$. For all k it is clear that the power of p_i appearing in m_k is exactly α_i , for all i . (All the nonconstant terms are divisible by higher powers of p_i , but the constant term is not.) Therefore $|m_k| = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell} = |f(0)|$, because no other primes can divide m_k by assumption.

But this is absurd: for sufficiently large k , $|m_k| > |f(0)|$. So we have a contradiction. \square