Math 129, HW 1

Bryden Cais

February 13, 2002

1 Finite Fields

1. If $p \neq 2$ and $x \in k$ is a square, then $x\ a^2$ for some $a \in k$. Thus, $x^{(q-1)/2} = a^{q-1} = 1$. Conversely, let r generate k^*. Then we have $x = r^b$ for some b, and thus $x^{(q-1)/2} = r^{b(q-1)/2} = 1$. Since r has order $q-1$, we conclude that $(q-1)|b(q-1)/2$ so that b is even and x is a square.

2. If $p = 2$ then for every $x \in k$ one has $x^{2^n} = \left(x^{2^{n-1}}\right)^2 = x$, so that x is a square.

3. First we handle the case that -1 is not a square in $\mathbf{F}_q$. Define $f_x : \mathbf{F}_q \longrightarrow \mathbf{F}_q$ for any $x \in \mathbf{F}_q$ by $f_x(y) := x^2 + y^2$. Notice that if $f_{x_1}(y) = f_{x_2}$ for some y then $x_1 = \pm x_2$ since we are working over a field. Thus, for any x, f_x takes on $(q-1)/2$ distinct values. Now let $S_x = \{f_x(y) : y \in \mathbf{F}_q\}$. Suppose that $S_{x_1} = S_{x_2}$ as sets. Then there exist $a,\ b \in \mathbf{F}_q$ such that $x_1^2 = x_2^2 + a^2$, and $x_1^2 + b^2 = x_2^2$. Hence, we have $a^2 = -b^2$. If $b \neq 0$ then -1 is a square. Since we have supposed that it is not, we must have $b = 0$, and therefore that $x_1 = \pm x_2$. Thus, if $x_1 \neq \pm x_2$ then the sets $S_{x_1},\ S_{x_2}$ are distinct. Since there are $(q-1)/2$ distinct sets and $(q-1)/2$ elements per set, we see that the S_x cover $\mathbf{F}_q$, and therefore that every element of $\mathbf{F}_q$ is the sum of two squares.

   Now we take care of the case that -1 is a square in $\mathbf{F}_q$. If $x \in \mathbf{F}_q$ is already a quadratic residue (=QR) we are done. So suppose that it is not. Now if $x + 1$ is a QR, then $x = a^2 - 1$, but since -1 is a square, we are done here too. So suppose that both $x,\ x+1$ are QNR's (quadratic non-residues). Then $x(x+1) = x^2 + x$ is a QR and we have $x = b^2 - x^2$ for some $b \in \mathbf{F}_q$, which, again since -1 is a QR, shows that x is the sum of two squares.

2 Sums of Two Squares

1. Since every square is 0 or 1 modulo 4, the sum of any two squares is $0,\ 1$, or 2 modulo 4 and hence never 3.

2. For any $\alpha,\ \beta \in \mathbf{Z}[i]$ with $\beta \neq 0$, we must show that there exists γ with $\alpha = \gamma\beta+\epsilon$ where $N(\epsilon) < N(\beta)$. This is clearly equivalent to finding some $\gamma \in \mathbf{Z}[i]$ such that $N(\alpha/\beta - \gamma) < 1$. Now $\mathbf{Z}[i]$ forms a lattice in $\mathbf{C}$ and α/β lies somewhere inside a fundamental domain of this lattice (posibly on the boundary.) Hence, the closest lattice point to α/β is not more than half the length of the diagonal of a fundamental cell away. Since $N(\alpha)$ clearly gives the square of the distance of α from the origin, we have that there exists some lattice point γ such that $N(\alpha/\beta-\gamma) < (\sqrt{2}/2)^2 < 1$, as required.

3. If $\alpha \in R$ and $N(\alpha) = 1$ then $\alpha\bar{\alpha} = 1$ so that $\alpha \in R^*$. Conversely, if $\alpha \in R^*$ then there exists some $\beta \in R^*$ so that $\alpha\beta = 1$. Since N is multiplicitave, this gives $N(\alpha)N(\beta) = 1$. Since $N(\alpha)$ must be a nonnegative integer, we clearly have $N(\alpha) = 1$. Thus R^* consists of all those elements of norm 1. Since $N(a+bi) = a^2+b^2$ and $a,\ b \in \mathbf{Z}$, we see that $a = \pm 1,\ b = \pm 1$, and $R^* = \{1, -1, i, -1\}$.

4. If $\alpha \in R$ is reducible, say $\alpha = \beta\gamma$ then $N(\alpha) = N(\beta)N(\gamma)$ is not prime (since neither β nor γ are units, their norms cannot be units in $\mathbf{Z}$. For part b, notice that if $\alpha = a+bi$ then $N(\alpha) = a^2+b^2$ is the sum of two squares and hence if $\alpha = \beta\gamma$ and $N(\alpha) = p^2$ where $p \equiv 3 \bmod 4$ we either have $N(\beta) = p$ or $N(\beta) = 1$ or $N(\beta) = p^2$. The first case is impossible by item 1 and the above, so we conclude that one of $\beta,\ \gamma$ is a unit and the other has norm p^2. Thus, α is irreducible.

5. If $p \equiv 3 \bmod 4$ then $N(p) = p^2$ so we are in case b above, which shows that p is irreducible in R. Now if $p \equiv 1\ mathrmmod\ 4$ then there exists some x and some n such that $x^2+1 = np$ (by the first problem). Hence, $p|(x-i)(x+i)$, but it cannot divide either $x-i$ or $x+i$ since it does not divide i. Thus, p cannot be prime in R (since R is Euclidean and hence a PID). Thus we can write $p = \alpha\beta$ for some $\alpha,\ \beta \in R$ neither of which is a unit. This forces $N(\alpha) = p$ (since it divides p^2 and cannot be 1 or p^2). Thus, $p = N(\alpha)$ as required. Moreover, α must be irreducible since if it were not, we would have $p = N(\alpha) = N(\beta)N(\gamma)$, and p is prime. Also, $\alpha,\ \bar{\alpha}$ are not associated since if they were, we would have $a = \pm b$ where $\alpha = a+bi$, whence $a|p$, requiring $a = 1$, which is clearly impossible unless $p = 2$. Finally, if $p = 2$ then it is trivial that $p = -i(1-i)^2$. To see that $1-i$ is irreducible, notice that its norm is 2, a prime.

6. We thus see that a set of irreducible elements of R is

   (a) $1+i$

   (b) $a+bi$ with $a^2+b^2 = p \equiv 1 \bmod 4$.

   (c) $p \equiv 3 \bmod 4$

   where p is a prime in Z.

7. The main theorem now follows easily. It is clearly enough to show that any square free integer n is the sum of two squares iff it is the product of primes congruent to 1 mod 4. In one direction, if n is the product or primes $p_1,\ p_2, \ldots p_r$ all congruent to 1 mod 4 then we have $p_i = \alpha_i\bar{\alpha_1}$ for each i, (for some α_i) and hence $n = N(\alpha_1\alpha_1\cdots\alpha_r)$ is the sum of two squares. Conversely, if n is the sum of two squares, we have $n = N(a+bi)$ for some $a+bi \in R$. Thus, if any prime $p \equiv 3 \bmod 4$ divides n, it divides a and b since it is also prime in R. As a result, p^2 divides n, a contradiction since we assumed n to be squarefree. This proves the main result.

8. Let us take $p = 577$. It is not hard to see that $577 = 24^2 + 1^2$.

9. Let $n = 685 = 5 \cdot 137 = (2-i)(2+i)(11+4i)(11-4i)$. Hence, $n = N((2-i)(11+4i)) = N((2-i)(11-4i)) = N((2+i)(11+4i)) = N((2+i)(11-4i))$ is expressible as the sum of two squares in $4 \cdot 2$ ways. That is: $n = (\pm 18)^2 + (\pm 19)^2 = (\pm 26)^2 + (\pm 3)^2$. We could have also deduced this from Jacobi's formula, $r_2(n) = 4\left(\sigma_1(n) - \sigma_3(n)\right)$.

3 $\mathbf{Z}[\omega]$ with $\omega = e^{2\pi i/3}$

1. Let $\alpha,\ \beta \in R = \mathbf{Z}[\omega]$, with $\beta \neq 0$, and define $N(\alpha)$ by $N(\alpha) = \alpha\bar{\alpha}$. Since every element of R has the form $a + b\omega$ (since $\omega^2 + \omega + 1 = 0$,) we may write $\alpha/\beta = \alpha\bar{\beta}/N(\beta) = r + q\omega$ for some $r,\ q \in \mathbf{Q}$. It is therefore possible to find integere $x,\ y$ such that $|x - r| \leq 1/2,\ |y - q| \leq 1/2$. We then have $N(\alpha/\beta - (x+y\omega)) = ((r-x)+(q-y)\omega)((r-x)+(q-y)\omega^2) = (r-x)^2 - (r-x)(q-y) + (q-y)^2 \leq 1/4+1/4+1/4 = 3/4 \leq 1$. Just as in our proof for $\mathbf{Z}[i]$, this shows that R is Euclidean.

2. The units of R are those elements of R on the unit circle. That is, $a + b\omega$ is a unit iff $a^2 - ab + b^2 = (a - b/2)^2 + 3b^2/4 = 1$, or $(2a-b)^2 + 3b^2 = 4$. It is obvious that the only solutions to this equation are $(a,b) = (\pm 1, 0),\ (0, \pm 1),\ (1,1),\ (-1,-1)$, corresponding to $\pm 1,\ \pm\omega,\ \pm(1+\omega)$, that is, the sixth roots of unity.

3. We have $(1-\omega)(1-\omega^2) = (1-\omega)(2+\omega) = 3$.

4. Notice that $N(4-\omega) = N(5+\omega) = 21 = -(1-\omega)(2+\omega)(2+3\omega)(1+3\omega)$. From this, it is easy to find that $4 - \omega = -\omega(1-\omega)(2+3\omega)$, and hence that $5 + \omega = 4 - \omega^2 = \omega^2(2+\omega)(1+3\omega)$. It is clear that none of the primes in the respective decompositions are associates, so that the $4 - \omega$ and $5 + \omega$ are relatively prime.

4 $\mathbf{Z}[\sqrt{-5}]$ is not a UFD

1. Here the norm of $a + b\sqrt{-5}$ is $a^2 + 5d^2$. If $\alpha \in \mathbf{Z}[\sqrt{-5}] = R$ is a unit, then $N(\alpha)$ must be 1 since it is positive and divides 1. But clearly, we must then have $b = 0$ whence $a = \pm 1$ are the only units.

2. It is obvious that $21 = 3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5}) = (4+\sqrt{-5})(4-\sqrt{-5})$.

3. It follows that R is not a UFD since $3,\ 7,\ (1 \pm 2\sqrt{-5}),\ (4 \pm \sqrt{-5})$ are all irreducibles. For if $7 = \alpha\beta$ then $49 = N(\alpha)N(\beta)$. If $\alpha,\ \beta$ are not units, we then have $N(\alpha) = 7 = a^2 + 5b^2$ for some integers $a,\ b$. Clearly, $b^2 < 1$. But $b \neq 0$ since 7 is not a square, while $b^2 \neq 1$ since 2 is not a square. Hence 7 is irreducible. Similarly, 3 is irreducible since it is less than 5 and not a square. Now if $\alpha | (1 \pm 2\sqrt{-5})$ in R then $N(\alpha)|21$ in $\mathbf{Z}$. But we have shown that there is no $\alpha \in R$ with norm 3 or 7 and hence $(1 \pm 2\sqrt{-5})$ must be prime. Similarly $(4 \pm \sqrt{-5})$ are both prime too. This shows that 21 may be factored in 3 different ways, since none of the irreducibles above are assoiates (since the only units are ± 1.) Hence, R is not a UFD.

5 Divisibility in $\mathbf{Z}[X]$

1. Suppose that $x + a = p(x)q(x)$ were reducible. Then clearly, $\deg(p) = 1$ and $\deg(q) = 0$ (interchanging $p,\ q$ if necessary.) Say $p = bx + c,\ q = d$. Then $bd = 1$ so that $b, d = \pm 1$, viz q is a unit. Hence $x + a$ is irrducible for any a.

2. If a degree 2 monic polynimial $p(x)$ is reducible, we clearly must have $p(x) = (x+a)(x+b)$ since p is monic. Hence p has two roots in $\mathbf{Z}$. Similarly is p is reducible of degree 3 then it is either the product of three linear factors or of a linear factor and an irreducible quadratic factor. In either case, p must be divisible by a monic degree 1 polynomial and hence has a root in $\mathbf{Z}$. Thus, if p has no roots in Z and is monic of degree 2 or 3, it must be irreducible.

3. Suppose that $f \in \mathbf{Z}[X]$ satisfies the criterion for the irreducible p. Then the reduction of f modulo p is $\bar{f} = \bar{a_n}X^n$. If f is reducible, then $f = gh$ for some $g,\ h \in \mathbf{Z}[X]$. Thus, $\bar{g}\bar{h} = \bar{a_n}X^n$ so that p divides every coefficient of g and h except for the leading coefficient. In particular, this implies that p^2 divided the constant term of f. But we know that this is not true, and hence f is irreducible.

6 Comments

I really liked the explicit nature of this problem set and thought that it complemented class well. I thought that having many small problems was an excellent idea. I do feel that the problem set was a bit long, however, and think that this might become a difficulty as the material proresses. Again, I emphasize that I really liked the explicit nature of the problems.