Math 113H

May 24, 1991

1. *Use quadratic reciprocity to determine whether or not 17 is a square mod 31.* By quadratic reciprocity, $\left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{-3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1$.

2. *Write $x^6 + 18x^5 - 4x^3 + 2x + 22$ as a product of irreducible polynomials over J_2.* The polynomial becomes x^6 over J_2. Since x is irreducible, we have answered the question.

3. *Write $x^6 + 18x^5 - 4x^3 + 2x + 22$ as a product of irreducible polynomials over* $\mathbf{Q}$. It's an Eisenstein polynomial for the prime $p = 2$, and therefore already irreducible.

4. *Write 17 as a product of irreducible elements in the ring* $\mathbf{Z}[i]$. We have $17 = (4 + i)(4 - i)$. The two factors are irreducible because their norms are 17, which is prime.

5. *Find the minimal polynomial for $\sqrt{2} + \sqrt{3}$ over $\mathbf{Q}$ and show that it is irreducible over* $\mathbf{Q}$. Let $x = \sqrt{2} + \sqrt{3}$. Then $(x - \sqrt{3})^2 = 2$, which gives $x^2 + 1 = 2\sqrt{3}x$. Squaring and collecting terms gives $x^4 - 10x^2 + 1 = 0$. The easiest way to know that this is irreducible is to prove that $\mathbf{Q}(\sqrt{2} + \sqrt{3})$ has degree 4 over $\mathbf{Q}$ by showing that $\mathbf{Q}(\sqrt{2} + \sqrt{3})$ contains the two distinct quadratic subfields $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{3})$, and so must have degree no smaller than 4 over $\mathbf{Q}$.

6. *Let I be a left ideal of a ring R which contains $rs - sr$ for all $r, s \in R$. Show that I is a 2-sided ideal.* We have to show that I is a right ideal. Take $i \in I$ and $r \in R$; we must show that $ir \in I$. But $ri = ir + (ri - ir)$ is the sum of two elements of I, and therefore lies in I.

7. *Let N be a normal subgroup of a group G. Suppose that the order of N is 5 and that G has odd order. Prove that N is contained in the center of G.* Consider the action of G on N by conjugation. This action amounts to a homomorphism $G \to \operatorname{Aut} N$. The target group has order 4, whereas G has odd order. Hence the homomorphism is trivial. This means that N lies in the center of G.

8. *Let G be a subgroup of the additive group of real numbers such that G has only finitely many elements in each closed interval $[a, b]$. Prove that G is cyclic.* If $G = 0$, then G is cyclic. If not, G contains some positive number. The hypothesis then implies that G contains a smallest positive number g. Indeed, if b is a positive number in G, then $G \cap [0, b]$ is finite, so there are at most finitely many elements of G which are smaller than b; we can take g to be the smallest of those. We now see in a standard manner than G is the cyclic group generated by g: Take $x \in G$, and choose $n \in \mathbf{Z}$ such that $ng \le x < (n + 1)g$. Then $0 \le x - ng < g$, and this implies $x = ng$ by the choice of g.

9. *Let $N = 561 = 3 \cdot 11 \cdot 17$. Prove the congruence $a^N \equiv a \pmod{N}$ for all integers a.* By unique factorization, it suffices to prove that $a^N - a$ is divisible by each of 3, 11, 17. Take 11, for example. Then $a^N - a$ is certainly divisible by 11 if a is. Thus, we can assume that a is prime to 11, in which case the congruence to be proved is $a^{560} \equiv 1 \pmod{11}$. By "Fermat's Little Theorem," $a^{10} \equiv 1 \pmod{11}$, so that the desired result follows because 10 divides 560. Similarly, $2 = 3 - 1$ divides 560, and $16 = 17 - 1$ divides 560.

10. *Let g be an element of a finite group G, and let $\sigma\colon G \to G$ denote the permutation $x \mapsto gx$ of G. Express the sign of σ in terms of the order of g and the order of G.* Decompose the set G into disjoint cycles, relative to the permutation σ. Two elements x and y of G are in the same cycle if and only if $x = g^i y$ for some $i \in \mathbf{Z}$, i.e., if and only if x and y lie in the same right coset of $\langle g \rangle$ in G. The cycles thus have length equal to the order of $\langle g \rangle$, which is the order of g. The number of cycles is the index of $\langle g \rangle$ in G, which is $\operatorname{o}(G)/\operatorname{o}(g)$. The desired sign is $(-1)^n$, where $n = (\operatorname{o}(g) - 1)(\operatorname{o}(G)/\operatorname{o}(g))$.

11. Let $R = \mathbf{Z}[\sqrt{5}]$ be the subring of $\mathbf{R}$ consisting of numbers $a + b\sqrt{5}$, with $a, b \in \mathbf{Z}$. Define a "norm" $N\colon R \to \mathbf{Z}$ by $N(a + b\sqrt{5}) = a^2 - 5b^2$. *Prove that an element of R is a unit if and only if its norm is ± 1.* If r is a unit, then $rs = 1$ for some $s \in R$, which gives $N(r)N(s) = N(rs) = N(1) = 1$, and therefore $N(r) = \pm 1$. Conversely, if $r = a + b\sqrt{5}$ has norm ± 1, then an inverse for it in R is $\pm(a - b\sqrt{5})$. *Show that the group of units of R is infinite.* The number $r = 2 + \sqrt{5}$ is a unit. Since $r > 1$, we cannot have $r^n = 1$ for any positive integer n. *Show that no element of R has norm ± 2.* If $a^2 - 5b^2 = \pm 2$, then we have $\pm 2 \equiv a^2 \pmod 5$. However, neither $+2$ nor -2 is a square mod 5. *Show that the formula $a + b\sqrt{5} \mapsto (a + b \bmod 2)$ defines a ring homomorphism $\varphi\colon R \to J_2$.* We just have to check that φ is compatible with addition and with multiplication. This is straightforward; you have to use that 5 is odd. *Prove that the kernel of φ is not a principal ideal of R.* Let I be the kernel, and suppose that I is generated by r. Since $2 \in I$, 2 is a multiple of r. Hence $N(r)$ divides $N(2) = 4$. If $N(r) = \pm 1$, then r is a unit, so that $I = R$ and then φ is identically 0. But $\varphi(1) = 1$, so this is impossible. Also, $N(r) \neq \pm 2$. Therefore, $N(r) = \pm 4$. Hence, if $2 = rs$ (say), then s has norm ± 1 and must be a unit. Thus 2 generates I, which means in particular that every element of I is a multiple of 2. We see, finally, that this is false by considering $1 + \sqrt{5}$: it is an element of I which is not a multiple of 2.

12. *Let K be a finite field. Prove that the product of the non-zero elements in K is -1.* The case $K = J_p$ corresponds to Wilson's Theorem, which we proved in class from several perspectives. Most of the proofs that we gave for Wilson's Theorem carry over to the general case without significant change. For example, by pairing up elements $x \in K^*$ with their inverses, we see that the product to be computed collapses to the product of those $x \in K^*$ for which $x = x^{-1}$, i.e., for which $x^2 - 1 = 0$. If K has characteristic 2, then $x^2 - 1 = (x - 1)^2$, and $x = 1$ is the only solution to the equation $x = x^{-1}$. Hence the product is 1, which happens also to be -1, since $2 = 0$. If K has chararacteristic different from 2, then $x^2 - 1 = 0$ has the two distinct solutions $+1$ and -1, and the product of these numbers is the desired -1.

I hope that you have enjoyed this class—I certainly have. I will be teaching Math 114 in the spring '92 semester, and look forward to seeing you then, if not before. Meanwhile, have a great summer!