Math 503 Midterm Exam

Wed. Oct. 3, 2012

PLEASE BEGIN YOUR SOLUTION TO EACH PROBLEM 1–5 ON A NEW SHEET.

---

1. Let $p = 4d + 1$ be a prime number in the ring $\mathbb{Z}$ of integers.

(a) (2 points) Prove that every nonzero element x in the field $\mathbb{Z}/p$ satisfies $x^{4d} = 1$.

(b) (2 points) Prove that for some x as in (a), x^d is a solution of the equation $X^2 = -1$.

Hint: $X^{4d} - 1 = (X^{2d} + 1)(X^{2d} - 1)$.

Solution. (a) From a homework problem: in a finite field of cardinality q, any $x \neq 0$ satisfies $x^{q-1} = 1$. (In this problem, $q = 4d + 1$.) You could just quote this result, or reproduce the proof. *Alternatively,* it would be okay to use the theorem—that hasn't been covered yet in class, but that most of you must know—that in a group of order n, every element satisfies $x^n = 1$. (In this problem, the group is the multiplicative group of nonzero elements in $\mathbb{Z}/p$.)

(b) By the hint, every nonzero $x \in \mathbb{Z}/p$ is a root of $X^{2d} + 1$ or of $X^{2d} - 1$. If $f(X)$ is a polynomial of degree n over any field k, and $x_1, \ldots, x_m \in k$ are distinct roots, then $m \leq n$, because the degree-m polynomial $(X - x_1) \cdots (X - x_m)$ divides $f(X)$. In particular, $X^{2d} - 1$ has at most $2d$ roots, and so $X^{2d} + 1$ has at least (hence precisely) $2d$ roots in $\mathbb{Z}/p$.

---

2. (4 pts) Find a linear combination (with Gaussian integer coefficients) of the Gaussian integers $14 - 7i$ and $3 + i$ which divides them both.

Solution. (As was done in class on the morning of the exam) just apply the euclidean algorithm to $14 - 7i$ and $3 + i$ to get that their gcd is $2 - i = (14 - 7i) - (3 - 3i)(3 + i)$.

---

3. (a) (4 pts) Let $n > 2$ be an integer. Using that 2 divides n (respectively $1+n$) when n is even (respectively odd), show that in $\mathbb{Z}[\sqrt{-n}]$, 2 is irreducible but not prime.

(b) (2 pts) Is there any $n > 2$ such that $\mathbb{Z}[\sqrt{-n}]$ is a unique factorization domain? Justify your answer in one or two sentences. (You can quote any result proved in class.)

Solution. Suppose that in $\mathbb{Z}[\sqrt{-n}]$, $2 = \alpha\beta$ where neither α nor β is a unit. Then for the norm $N(a+b\sqrt{-n}) := a^2 + nb^2 \in \mathbb{Z}$, we have $N(\alpha) > 1$, $N(\beta) > 1$, and

$$4 = N(2) = N(\alpha)N(\beta),$$

whence $N(\alpha) = N(\beta) = 2$, which is impossible as $a^2 + nb^2$ can't be 2 if $n > 2$. Thus 2 is irreducible.

If n is even (resp. odd) then 2 divides $\sqrt{-n}\,.\sqrt{-n}$ (resp. $(1+\sqrt{-n})(1-\sqrt{-n})$), but 2 does not divide any of the factors in these products. Thus 2 is not prime.

(b) No, because in a UFD every irreducible element is prime.

In the next two problems, you will be graded for clarity of exposition in addition to correctness; so take your time and think carefully before writing.

4. (5 pts) Let R be a commutative ring, let $I \subset R$ be an ideal, and let $\pi\colon R \to \overline{R} := R/I$ be the canonical map. Let $f\colon R \to S$ be a homomorphism of rings such that $f(x) = 0$ for all $x \in I$. Prove carefully that there exists a unique ring-homomorphism $\bar{f}\colon \overline{R} \to S$ such that $\bar{f} \circ \pi = f$.

Solution. (Uniqueness.) Every $\bar{x} \in \overline{R}$ is of the form $\pi(x)$ for some $x \in R$. So if $g \circ \pi = f = \bar{f} \circ \pi$ then for all $\bar{x}$,

$$g(\bar{x}) = g(\pi x) = f(x) = \bar{f}(\pi x) = \bar{f}(\bar{x}),$$

i.e., $g = \bar{f}$. Thus $\bar{f}$ is unique, if it exists.

(Existence.) Set $\bar{x} := \pi(x)$ $(x \in R)$. Then

$$\bar{x} = \bar{y} \implies x - y \in I \implies f(x) - f(y) = f(x-y) = 0 \implies f(x) = f(y).$$

Therefore there is a map of sets $\bar{f}\colon \overline{R} \to S$ such that $\bar{f}(\bar{x}) = f(x)$ for all $x \in R$, i.e., $\bar{f} \circ \pi = f$. Let us check that this $\bar{f}$ is a ring-homomorphism.

For this note that

$$\bar{f}(\bar{x} + \bar{y}) = \bar{f}(\overline{x+y}) = f(x+y) = f(x) + f(y) = \bar{f}(\bar{x}) + \bar{f}(\bar{y}).$$

Similarly, $\bar{f}(\bar{x}\bar{y}) = \bar{f}(\bar{x})\bar{f}(\bar{y})$. Last, $\bar{1}$ is the identity in $\overline{R}$, and $\bar{f}(\bar{1}) = f(1) = 1_S$.

---

5. (6 pts) In an integral domain R, let x be an element such that

$$x = up_1^{e_1} p_2^{e_2} \dots p_m^{e_m} \quad \text{and} \quad x = vq_1^{f_1} q_2^{f_2} \dots q_n^{f_n},$$

where u and v are units, the p's and q's are primes in R, the e's and f's are positive integers, and if $i \neq j$, then p_i is not an associate of p_j and q_i is not an associate of q_j.

What can you say about the relation between these two factorizations? Formulate your answer with precision, and justify it by an inductive proof. (You may assume without proof that cancelation holds in R: if $cx = cy$ and $c \neq 0$ then $x = y$.)

Solution. (On the original exam I forgot to include the second line after the display; but fortunately almost everyone assumed it.)

We have $m = n$, and, after rearranging, $p_i \sim q_i$ and $e_i = f_i$ for all i.

(Here $\sim$ denotes the relation "is an associate of.")

More precisely, $m = n$, *and there is a permutation π of $\{1, 2, \dots, n\}$ such that for all i, $p_i \sim q_{\pi(i)}$ and $e_i = f_{\pi(i)}$.*

This can be proved by induction on the integer $|f| = f_1 + f_2 + \cdots + f_n$.

If $|f| = 0$ then x is a unit, and therefore $m = 0$.

If $|f| > 0$, then, since q_1 is prime and $q_1 | x$, therefore $q_1 | p_i$ for some i. Similarly, $p_i | q_j$ for some j. So q_1 divides the prime q_j, whence $q_1 \sim q_j$ and $j = 1$ and $q_1 = wp_i$ for some unit w. After rearranging, we may assume that $i = 1$. Applying the inductive hypothesis to the factorizations $uw^{-1} p_1^{e_1 - 1} p_2^{e_2} \dots p_m^{e_m}$ and $vq_1^{f_1 - 1} q_2^{f_2} \dots q_n^{f_n}$ of x/q_1, we see that the assertion holds for $|f|$.

Note that this argument is essentially the same as the one in section **24** of Clark.