Wed May 7 22:18:00 2003 : Hi could you opst solutions to 8.2.7, 8.3.6,8.3.7, 9.4.3 ? Thanks

**Problem 7 of §8.2:** Suppose that $R$ is a Bezout domain. Let $a$ and $b$ be elements of $R$ and let $d$ be a generator of the ideal $(a, b)$. Then $d$ is a greatest common divisor of $a$ and $b$ by Proposition 2 on page 275. Since $d \in (a, b)$, $d$ can be written in the form $ax + by$. Conversely, suppose that every pair of elements $a$ and $b$ have a greatest common divisor $d$ of the form $ax + by$. Let $a$ and $b$ be given elements and let $d = ax + by$ be a common divisor. Then $d$ lies in $(a, b)$ because this ideal consists of all $ax + by$ as $x$ and $y$ run through $R$. Further, $a$ and $b$ each are multiples of $d$, so they lie in $(d)$. Thus we have $(a, b) \subseteq (d)$ and $(d) \subseteq (a, b)$, so $(a, b) = (d)$ is principal. This gives part (a).

Part (b) is proved by the same argument explained in my solution to Problem 4 of §8.2. (This solution was posted after the previous assignment was handed in.)

For part (c), we have to understand that every element of $F$ can be written $a/b$ with $a, b \in R$ and $b$ non-zero. Let $d = ax + by$ be a greatest common divisor of $a$ and $b$. Write $a = da'$, $b = db'$ with $a', b' \in R$. Then $a/b = a'/b'$. Moreover, we have $1 = a'xc + b'y$, and it follows from this equation that $a'$ and $b'$ are relatively prime. (Anything that divides $a'$ and $b'$ divides 1 and must therefore be a unit.)

**Problem 6 of §8.3:** For part (a), we note that $i$ is congruent to $-1$ mod $(1+i)$, so that $a + bi \equiv a - b \bmod (1 + i)$. This remark establishes the surjectivity of the natural map $\mathbf{Z} \to \mathbf{Z}[i]/(1 + i)$ (given by $a \mapsto a \bmod (1 + i)$). The kernel of this map contains $(2) = 2\mathbf{Z}$ since $2 = (1 + i)(1 - i)$; the kernel does not contain 1 since $1 = \alpha \cdot (1 + i)$ would imply the impossible equality of integers $1 = N(1) = N(\alpha)N(1 + i) = 2N(\alpha)$. Hence the kernel is precisely $2\mathbf{Z}$ and we get an isomorphism $\mathbf{Z}/2\mathbf{Z} \xrightarrow{\sim} \mathbf{Z}[i]/(1 + i)$.

For part (b), to show that $\mathbf{Z}[i]/(q)$ is a field, it suffices to show that $q$ is irreducible, since we know that irreducible elements in PIDs generate maximal ideals. If $q$ is not irreducible, it may be written as a product $\alpha\beta$ where $\alpha$ and $\beta$ are non-units. We then get $q^2 = N(q) = N(\alpha)N(\beta)$. The numbers $N(\alpha)$ and $N(\beta)$ can't be 1 because the only elements of norm 1 are the units $\pm 1, \pm i$. Hence both norms are forced to be $q$. As we have seen in class, though, numbers that are

3 mod 4 cannot be written as the sum of two squares in $\mathbf{Z}$. Hence there are no elements of $\mathbf{Z}[i]$ of norm $q$, so there is no factorization $q = \alpha\beta$. Conclusion: $q$ is indeed irreducible. We were asked to establish also that $\mathbf{Z}[i]/(q)$ has $q^2$ elements. This is obvious because any $a + bi \in \mathbf{Z}[i]$ is congruent mod $q$ to precisely one $x + iy$ with $0 \le x, y \le q - 1$.

For part (c), we recall that $p$ can be written as a sum $a^2 + b^2$ in $\mathbf{Z}$ and therefore as a product $(a + bi)(a - bi)$ in $\mathbf{Z}[i]$. Let $\pi = a_b i$ and $\bar{\pi} = a - bi$. (The "bar" here is complex conjugation.) These two elements have prime norm, so they're irreducible. (If they factored non-trivially, their norms would factor non-trivially. . . .) The two ideals $I = (a + bi)$ and $J = (a - bi)$ are maximal because they're generated by irreducible elements, so they're co-maximal unless they are equal. If $I = J$, then $a + bi$ divides $a - bi$ and vice versa, so the two elements are associates (i.e., are equal up to multiplication by units). This is certainly impossible for various reasons: they're not equal up to sign because $a$ and $b$ are both non-zero, and they're not equal up to multiplication by $\pm i$ because $a$ and $b$ have different parity. Hence it's true that $\mathbf{Z}[i]/(p)$ is isomorphic to the product of the two quotient rings $\mathbf{Z}[i]/(\pi)$ and $\mathbf{Z}[i]/(\bar{\pi})$. Now $\mathbf{Z}[i]/(p)$ clearly has $p^2$ elements (just as $\mathbf{Z}[i]/(q)$ had $q^2$ elements in the previous part), so the two fields $\mathbf{Z}[i]/(\pi)$ and $\mathbf{Z}[i]/(\bar{\pi})$ are forced each to have order $p$. (They're fields because we've divided out by maximal ideals.)

**Problem 7 of §8.3:** If $\pi$ is irreducible and $n$ is non-negative, then $(\pi^{n+1})$ is an ideal of $\mathbf{Z}[i]$ that is contained in $(\pi^n)$. Consider the map (of additive groups) $\mathbf{Z}[i] \to (\pi^n)/(\pi^{n+1})$ that sends $\alpha$ to $\pi^n\alpha$. This is a homomorphism of groups whose kernel is the set of $\alpha$ such that $\alpha\pi^n$ is divisible by $\pi^{n+1}$ in $\mathbf{Z}[i]$. That set is clearly the set of $\alpha$ that are divisible by $\pi$ (unique factorization). By one of the numbered isomorphism theorems (the first one, I think), we get an isomorphism $\mathbf{Z}[i]/(\pi) \xrightarrow{\sim} (\pi^n)/(\pi^{n+1})$. This tells us that the index $\big((\pi^n) : (\pi^{n+1})\big)$ is equal to the index of $(\pi)$ in $\mathbf{Z}[i]$.

More generally, the same argument with $\pi^n$ replaced by an arbitrary non-zero element $\beta$ of $\mathbf{Z}[i]$ shows that $\mathbf{Z}[i]/(\pi)$ is isomorphic as an additive group to $(\beta)/(\pi\beta)$. Hence the index of $(\beta\pi)$ in $(\beta)$ agrees with the index of $(\pi)$ in $\mathbf{Z}[i]$. Hence $(\mathbf{Z}[i] : (\beta\pi)) = (\mathbf{Z}[i] : (\beta))((\beta) : (\beta\pi)) = (\mathbf{Z}[i] : (\beta))(\mathbf{Z}[i] : (\pi))$. It follows by induction that $(\mathbf{Z}[i] : (\alpha)) = \prod_i (\mathbf{Z}[i] : (\pi_i))$ if $\alpha = \pi_1\pi_2 \cdots \pi_n$ is the product of $n$ irreducible elements of $\mathbf{Z}[i]$. Note that $(\mathbf{Z}[i] : (\alpha))$ is the order of the quotient ring $\mathbf{Z}[i]/(\alpha)$.

To prove that $(\mathbf{Z}[i] : (\alpha))$ has order $N(\alpha)$, we can start by remarking that both numbers are 1 when $\alpha$ is a unit. If not, $\alpha$ is a product $\pi_1\pi_2\cdots\pi_n$, and we are reduced to proving that $(\mathbf{Z}[i] : (\pi)) = N(\pi)$ when $\pi$ is irreducible.

For this, we first note that $\pi$ divides $\pi\bar{\pi} = N(\pi)$, which is an integer $> 1$. (The norm can't be 1 because then $\pi$ would be one of the units $\pm 1, \pm i$.) Hence, in $\mathbf{Z}[i]$ $\pi$ divides some integer. Therefore $\pi$ divides some prime number because it is irreducible. Hence $\pi$ is one of the irreducible elements that were discussed in the previous problem (#6). In all cases in that problem, we saw that the number of elements in $\mathbf{Z}[i]/(\pi)$ equaled the norm of $\pi$, as we sought to show.

**Problem 3 of §9.4:** Let $p(x)$ be the given polynomial of degree $n$, and suppose that $p(x)$ factors as $a(x)b(x)$, where $a$ and $b$ are non-constant. For each $i$ between 1 and $n$, we have $a(i)b(i) = -1$, so that one of $a(i), b(i)$ is $+1$ and the other is $-1$. Hence $a(x) + b(x)$ vanishes at all integers between 1 and $n$. Since $a + b$ has degree $< n$, we have $a(x) = -b(x)$, so $p(x) = -a(x)^2$. This is impossible because $p(x)$ could then take only non-positive values, whereas $p(x)$ is visibly positive if $x$ is large and positive.