Student: Cheng Yu (Jade)

Math 412

Exam #1

July 13, 2010

Exam #1

Question 1: Solve $11x = 1 \bmod 41$

Answer: We first compute the GCD of 11 and 41.

		3	1	2	1	2
0	1	3	4	11	15	41
1	0	1	1	3	4	11

So $\gcd(11, 41) = 15 \times 11 - 4 \times 41 = 1$.

$$11x = 1 \bmod 41$$

$$\Rightarrow 15 \times 11x = 15 \times 1 \bmod 41$$

$$\Rightarrow (4 \times 41 + 1)x = 15 \bmod 41$$

$$\Rightarrow x = 15 \bmod 41 .$$

Question 2: Factor 102 into primes in $\mathbb{Z}[i]$.

Answer: Gaussian integers form a unique factorization domain. In other words, for any Gaussian integer, in the form of $a + bi$, where $a, b \in \mathbb{Z}$, there is a unique decomposition of product of Gaussian primes. Gaussian primes are Gaussian integers $a + bi$ satisfying one of the following properties. If both a and b are nonzero then, $a + bi$ is a Gaussian prime if and only if $a^2 + b^2$ is an ordinary prime. If $a = 0$, then $a + bi$ is a Gaussian prime if and only if $|b|$ is an ordinary prime and $|b| = 3 \bmod 4$. If $b = 0$, then $a + bi$ is a Gaussian prime if and only if $|a|$ is an ordinary prime and $|a| = 3 \bmod 4$.

$$102 = 2 \times 3 \times 17$$

$$= (1 + i) \times (1 - i) \times 3 \times 17$$

$$= (1 + i) \times (1 - i) \times 3 \times (4 + i) \times (4 - i) .$$

Question 3: Prove that if $\mathbb{F}$ is a field and $p(x) \in \mathbb{F}[x]$, then $x - a$ divides $p(x)$ if and only if $p(a) = 0$.

Answer: We first prove that $x - a$ divides $p(x) \in \mathbb{F}[x]$ derives $p(a) = 0$.

$$x - a \text{ divides } p(x)$$

$$\Rightarrow p(x) = (x - a) \cdot q(x), \qquad \text{where } q(x) \in \mathbb{F}[x]$$

$$\Rightarrow p(a) = (a - a) \cdot q(a)$$

$$\Rightarrow p(a) = 0 \cdot q(a)$$

$$\Rightarrow p(a) = 0\,.$$

We now prove that $p(a) = 0$ derives $x - a$ divides $p(x)$. The Polynomial Division Algorithm states, let $f(x)$ and $g(x)$ be two nonzero polynomials in $\mathbb{F}[x]$, where $\mathbb{F}$ is a field and $g(x)$ is a nonconstant polynomial. Then there exist unique polynomials $q(x); r(x) \in \mathbb{F}[x]$ such that the following equation holds, where either $\deg r(x) < \deg g(x)$ or $r(x)$ is the zero polynomial.

$$f(x) = g(x)q(x) + r(x)$$

Our $g(x)$ is $x - a$, $f(x)$ is $p(x)$. Since $\deg g(x) = 1$, $r(x)$ has to be a constant or zero polynomial. Therefore we have the following.

$$p(x) = (x - a)q(x) + r(x)$$

$$= (x - a)q(x) + c$$

$$p(a) = 0$$

$$\Rightarrow p(a) = (a - a)q(a) + c = 0$$

$$\Rightarrow c = 0$$

$$\Rightarrow p(x) = (x - a)q(x)\,.$$

At this point, we've shown that if $\mathbb{F}$ is a field and $p(x) \in \mathbb{F}[x]$, then $x - a$ divides $p(x)$ if and only if $p(a) = 0$.

Question 4: Using the previous problem, explain carefully how you would construct a field of order 125.

Answer: I would construct the following set and prove that it is a field, and it have an order of 125.

$$\left(\mathbb{Z}/5\mathbb{Z}\right)[x]/(x^3 + x + 1)\,.$$

The set of all polynomials with coefficients in the field $\mathbb{F}$ forms a commutative ring denoted as $\mathbb{F}[X]$. $\mathbb{Z}/5\mathbb{Z}$ forms a commutative ring, and since 5 is a prime number, $\mathbb{Z}/5\mathbb{Z}$ is also a field, with a multiplicative identity, 1. Therefore $(\mathbb{Z}/5\mathbb{Z})[x]$ forms a commutative ring.

As we've proved in the previous problem that $f(x) = x^3 + x + 1 = 0$ is a necessary and sufficient condition for $f(x)$ divides $(\mathbb{Z}/5\mathbb{Z})[x]$. So $(\mathbb{Z}/5\mathbb{Z})[x]/(x^3 + x + 1)$ forms a quotient ring if and only if $f(x) = 0$. $f(x) = x^3 + x + 1$ is irreducible over $\mathbb{Z}/5\mathbb{Z}$. In other words, $f(x) = 0$ has no root in $\mathbb{Z}/5\mathbb{Z}$. We can verify this by plugging in all 5 elements of $\mathbb{Z}/5\mathbb{Z}$ in $f(x)$: $f(0) = 1, f(1) = 3, f(2) = 1, f(3) = 1$ and $f(4) = 4$. So $f(x)$ is a maximal ideal. The quotient ring $(\mathbb{Z}/5\mathbb{Z})[x]/(x^3 + x + 1)$ is, therefore, a field.

The elements in this field can be written as $a + bx + cx^2$, where $x^3 + x + 1 = 0$, and $a, b, c \in \mathbb{Z}/5\mathbb{Z}$. There are $5 \times 5 \times 5 = 125$ combinations of selecting $a, b,$ and c, the order of field, $(\mathbb{Z}/5\mathbb{Z})[x]/(x^3 + x + 1)$, is therefore 125.

Question 5: Given ideals I, J in a commutative ring R with 1, define $IJ = \{xy : x \in I, y \in J\}$. Prove that IJ is an ideal with $IJ \subseteq I \cap J$.

Answer: We first prove that $IJ = \{xy : x \in I, y \in J\}$ is an ideal. For an arbitrary ring $(R, +, \cdot)$, let $(R, +)$ be the underlying additive group. A subset I is called a two-sided ideal (or simply an ideal) of R if $(I, +)$ is a subgroup of $(R, +)$ and for all x in I and for all r in R, $x \cdot r$ and $r \cdot x$ are in I.

It is clear that $(IJ, +)$ is a subgroup of $(R, +)$. It is closed under addition; the addition operation is associative with the an identity 0_R; the inverse of any element xy is $-xy$, where $-x \in I, y \in J$.

Let $r \in R$, $a_{ij} \in IJ$, $a_i \in I$, and $a_j \in J$, where $a_{ij} = a_i a_j$, $a_i r = r a_i = a_i'$, and $a_j r = r a_j = a_j'$. The last assumption is based on the fact that R is a commutative ring hence $a_i r = r a_i$ and $a_j r = r a_j$.

$$a_{ij} r = a_i a_j r$$

Since J is an ideal, $a_j r = a_j' \in J$

$$\Rightarrow a_{ij} r = a_i a_j' \in IJ$$

$$r a_{ij} = r a_i a_j$$

Since I is an ideal, $r a_i = a_i' \in I$

$$\Rightarrow r a_{ij} = a_i' a_j \in IJ$$

Since R is commutative and $IJ \subseteq R$

$$\Rightarrow a_{ij} r = r a_{ij}$$

$$\Rightarrow a_{ij} r = r a_{ij} \in IJ\,.$$

Therefore, we've shown that IJ is an ideal in R. Now we need to show $IJ \subseteq I \cap J$.

Since I is an ideal in $R, a_i \in I$ and $a_j \in J \subseteq R$

$\Rightarrow a_i a_j = a_j a_i \in I$

Since J is an ideal in $R, a_j \in J$ and $a_i \in I \subseteq R$

$\Rightarrow a_i a_j = a_j a_i \in J$

$\Rightarrow a_{ij} = a_i a_j = a_j a_i \in I \cap J$

$\Rightarrow IJ \subseteq I \cap J$.

Any element $a_{ij} \in IJ$ is also an element in $I \cap J$, so $IJ \subseteq I \cap J$.

Question 6: Can the containment be proper in the preceding problem?

Answer: IJ is not a proper subset of $I \cap J$. The equivalent condition may satisfy. For example, let $1 \in I$ and $J = \{0\}$.

Since $1r = r1 = r \in I$ for all $r \in R$

$\Rightarrow I = R$, the unit ideal

Since $0r = r0 = 0 \in J$ for all $r \in R$

$\Rightarrow J$ is an ideal, the trivial ideal

$\Rightarrow IJ = \{xy : x \in I, y \in J\} = \{x0 : x \in I\} = \{0\}$

$\Rightarrow I \cap J = R \cap \{0\} = \{0\}$

$\Rightarrow IJ = I \cap J$.

But IJ and $I \cap J$ don't have to be equal. For example in the integer ring, $\mathbb{Z}$, $I = J = \langle 2 \rangle$.

$I = J = \langle 2 \rangle$

$\Rightarrow I \cap J = I = J = \langle 2 \rangle$

$\Rightarrow IJ = \langle 4 \rangle$

$\Rightarrow IJ \neq I \cap J$

$\Rightarrow IJ \subset I \cap J$.