

Math 3613
Second Exam
April 11, 2008

Name: _____

Be sure to explain carefully all details.

1. Definitions

- (a) (4 pts) What precisely do we mean when we say a is *congruent to b modulo n* (i.e. $a \equiv b \pmod{n}$)?
- (b) (5 pts) Suppose R is a set with two operations defined: “addition” $\oplus : R \times R \rightarrow R$ and “multiplication” $\otimes : R \times R \rightarrow R$ and “multiplication”. What additional properties are required so that R is a ring? (Hint: there are six additional required properties.)
- (c) (4 pts) What is an *integral domain*?
- (d) (4 pts) What is a *homomorphism* between two rings?
- (e) (4pts) What is the *greatest common divisor* of two polynomials over a field F ?
- (f) (4pts) What is an *irreducible polynomial*?

3. (15 pts) Prove that a unit in a commutative ring R cannot be a zero divisor.

4. (15 pts) Let R and S be rings and $f : R \rightarrow S$ a ring homomorphism. Prove that

$$f(R) = \{s \in S \mid s = f(r) \text{ for some } r \in R\}$$

is a subring of S .

5. (15 pts) Let p be a positive prime and let $R = \left\{x \in \mathbb{Q} \mid x = \frac{r}{p^i}, \text{ with } r, i \in \mathbb{Z}\right\}$. Prove that R is a subring of \mathbb{Q} . (You do not need to show that \mathbb{Q} is a ring.)

6. (15 pts) Let F be a field and $f, g \in F[x]$. Prove that f and g are associates if and only if $f|g$ and $g|f$.

7. (15 pts) Let F be a field, $f, g, h \in F[x]$ with f and g relatively prime. Suppose $h|f$. Prove that h and g are relatively prime.

Lemmas, Theorems, and Corollaries

1. CHAPTER 1

Theorem 1.1. (*THE DIVISION ALGORITHM*) Let a, b be integers with $b > 0$. Then there exists unique integers q and r such that

$$\begin{aligned} (i) \quad & a = bq + r \\ (ii) \quad & 0 \leq r < b \quad . \end{aligned}$$

Corollary 1.2. Let a, b be integers with $b \neq 0$. Then there exists unique integers q and r such that

$$\begin{aligned} (i) \quad & a = bq + r \\ (ii) \quad & 0 \leq r < |b| \quad . \end{aligned}$$

Theorem 1.3. Let a and b be integers, not both zero, and let $d = \text{GCD}(a, b)$. Then there exists (not necessarily unique) integers u and v such that

$$d = au + bv \quad .$$

Corollary 1.4. Let a and b be integers, not both zero, and let d be a positive integer. Then $d = \text{GCD}(a, b)$ if and only if d satisfies

$$\begin{aligned} (i) \quad & d \mid a \quad \text{and} \quad d \mid b \\ (ii) \quad & \text{if } c \mid a \text{ and } c \mid b, \text{ then } c \mid d \quad . \end{aligned}$$

Theorem 1.5. If $a \mid (bc)$ and $\text{GCD}(a, b) = 1$, then $a \mid c$.

Lemma 1.6. If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$, then

$$\text{GCD}(a, b) = \text{GCD}(b, r) \quad .$$

Theorem 1.7. Let p be an integer with $p \neq 0, \pm 1$. Then p is prime if and only if p has this property:

$$p \mid bc \quad \Rightarrow \quad p \mid b \quad \text{or} \quad p \mid c \quad .$$

Corollary 1.8. If p is prime and $p \mid a_1 a_2 \cdots a_n$, then p divides at least one of the a_i .

Theorem 1.9. Every integer n except $0, \pm 1$ is the product of primes

Theorem 1.10. (*THE FUNDAMENTAL THEOREM OF ARITHMETIC*) Every integer n except $0, \pm 1$ is a product of primes. This prime factorization is unique in the following sense: If

$$n = p_1 p_2 \cdots p_r \quad \text{and} \quad n = q_1 q_2 \cdots q_s$$

with each p_i, q_j prime, then $r = s$ (that is the number of factors is the same) and after reordering and relabeling the q_j 's

$$\begin{aligned} p_1 &= \pm q_1 \\ p_2 &= \pm q_2 \\ &\vdots \\ p_r &= \pm q_r \quad . \end{aligned}$$

Corollary 1.11. Every integer $n > 1$ can be written in one and only one way as

$$n = (p_1)^{s_1} (p_2)^{s_2} \cdots (p_r)^{s_r}$$

where the s_i are positive integers and the p_i are positive prime integers such that

$$p_1 < p_2 < \cdots < p_r \quad .$$

2. CHAPTER 2

Theorem 2.1. Let n be a positive integer. For all $a, b, c \in \mathbb{Z}$

- (i) $a \equiv a \pmod{n}$
- (ii) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$
- (iii) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

Theorem 2.2. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

- (i) $a + c \equiv b + d \pmod{n}$
- (ii) $ac \equiv bd \pmod{n}$.

Theorem 2.3. $a \equiv c \pmod{n}$ if and only if $[a] = [c]$.

Corollary 2.4. Two congruence classes modulo n are either disjoint or identical.

Corollary 2.5. There are exactly n distinct congruence classes modulo n ; namely, $[0], [1], [2], \dots, [n-1]$.

Theorem 2.6. If $[a] = [b]$ and $[c] = [d]$ in \mathbb{Z}_n , then

$$[a + c] = [b + d] \quad \text{and} \quad [ac] = [bd] \quad .$$

Theorem 2.7. For any classes $[a], [b], [c]$ in \mathbb{Z}_n ,

- (1) If $[a] \in \mathbb{Z}_n$ and $[b] \in \mathbb{Z}_n$, then $[a] \oplus [b] \in \mathbb{Z}_n$.
- (2) $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$.
- (3) $[a] \oplus [b] = [b] \oplus [a]$.
- (4) $[a] \oplus [0] = [a]$.
- (5) For each $[a] \in \mathbb{Z}_n$, the equation $[a] + X = [0]$, has a solution in \mathbb{Z}_n .
- (6) If $[a] \in \mathbb{Z}_n$ and $[b] \in \mathbb{Z}_n$, then $[a] \cdot [b] \in \mathbb{Z}_n$.
- (7) $[a] \cdot ([b] \cdot [c]) = ([a] \cdot [b]) \cdot [c]$.
- (8) $[a] \cdot ([b] \oplus [c]) = ([a] \cdot [b]) \oplus ([a] \cdot [c])$.
- (9) $[a] \odot [b] = [b] \odot [a]$.
- (10) $[a] \odot [1] = [a]$.

Theorem 2.8. If $p > 1$ is an integer, then the following properties are equivalent.

- (1) p is prime.
- (2) For any $[a] \neq [0]$ in \mathbb{Z}_p , the equation $[a][x] = [1]$ has a solution in \mathbb{Z}_p .
- (3) Whenever $[a][b] = [0]$ in \mathbb{Z}_p , then $[a] = [0]$ or $[b] = [0]$.

Corollary 2.9. Let a and n be integers with $n > 1$. Then $\text{GCD}(a, n) = 1$ if and only if the equation $[a][x] = [1]$ in \mathbb{Z}_n has a solution.

3. CHAPTER 3

Theorem 3.1. Let R and S be rings. Define addition and multiplication on $R \times S$ by

$$(r, s) + (r, s) = (r + r, s + s) \quad ,$$

$$(r, s)(r, s) = (rr, ss) \quad .$$

Then $R \times S$ is a ring. If R and S are both commutative, then so is $R \times S$. If R and S each has an identity, then so does $R \times S$.

Theorem 3.2. For any element a in a ring R , the equation $a + x = 0_R$ has a unique solution.

Theorem 3.3. If S is a subset of a ring R and

- (i) $a + b \in S$ whenever $a, b \in S$;
- (ii) $ab \in S$ whenever $a, b \in S$;
- (iii) $-a \in S$ whenever $a \in S$;

then S is a subring of R .

Theorem 3.4. If $a + b = a + c$ in a ring R , then $b = c$.

Theorem 3.5. For any elements a, b of a ring R :

- (a) $a \cdot 0_R = 0_R = 0_R \cdot a$
- (b) $a(-b) = -(ab) = (-a)b$

- (c) $-(-a) = a$
- (d) $-(a + b) = -a + (-b)$
- (e) $-(a - b) = -a + b$
- (f) $(-a)(-b) = ab$
- (g) If R has an identity 1_R , then $(-1_R)a = -a$

Theorem 3.6. Let R be a ring and let $a, b \in R$. Then the equation $a + x = b$ has the unique solution $x = b - a$.

Theorem 3.7. Let R be a ring with identity and $a, b \in R$. If a is a unit, then each of the equations

$$\begin{aligned} ax &= b \\ ya &= b \end{aligned}$$

has a unique solution in R .

Theorem 3.8. Let R be a commutative ring with identity. Then R is an integral domain if and only if in has this cancellation property:

Corollary 3.9. Every field R is an integral domain.

Theorem 3.10. Every finite integral domain R is a field.

Theorem 3.11. Let $f : R \rightarrow S$ be a homomorphism of rings. Then

- (i) $f(0_R) = 0_S$.
- (ii) $f(-r) = -f(r)$ for every $r \in R$.

Moreover, if R and S have identities and f is an isomorphism, then

- (iii) $f(1_R) = 1_S$.

4. CHAPTER 4

Theorem 4.1. If R is an integral domain and $f(x), g(x)$ are nonzero polynomials in $R[x]$, then

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)) \quad .$$

Corollary 4.2. If R is an integral domain, then so is $R[x]$.

Theorem 4.3. (The Division Algorithm in $F[x]$) Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0_F$. Then there exists unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

- (i) $f(x) = g(x)q(x) + r(x)$
- (ii) either $r(x) = 0_F$ or $\deg(r(x)) < \deg(g(x))$

Theorem 4.4. Let F be a field and $f(x), g(x) \in F[x]$, not both zero. Then there is a unique greatest common divisor $d(x)$ of $f(x)$ and $g(x)$. Furthermore, there exist (not necessarily unique) polynomials $u(x)$ and $v(x)$ such that

$$d(x) = f(x)u(x) + g(x)v(x) \quad .$$

Corollary 4.5. Let F be a field and $f(x), g(x) \in F[x]$, not both zero. A monic polynomial $d(x) \in F[x]$ is the greatest common divisor of $f(x)$, $g(x)$ if and only if $d(x)$ satisfies these conditions:

- (i) $d(x) \mid f(x)$ and $d(x) \mid g(x)$;
- (ii) If $c(x) \mid f(x)$ and $c(x) \mid g(x)$, then $c(x) \mid d(x)$.

Theorem 4.6. Let F be a field and $f(x), g(x), h(x) \in F[x]$. If $f(x) \mid g(x)h(x)$ and $f(x)$ and $g(x)$ are relatively prime, then $f(x) \mid h(x)$.

Theorem 4.7. Let F be a field. Then $f(x)$ is a unit in $F[x]$ if and only if $f(x)$ is a non-zero constant polynomial.

Theorem 4.8. Let F be a field and $p(x)$ a nonconstant polynomial in $F[x]$. Then the following conditions are equivalent:

- (1) $p(x)$ is irreducible.
- (2) If $b(x)$ and $c(x)$ are any polynomials such that $p(x) \mid b(x)c(x)$, then $p(x) \mid b(x)$ or $p(x) \mid c(x)$.
- (3) If $r(x)$ and $s(x)$ are any polynomials such that $p(x) = r(x)s(x)$, then $r(x)$ or $s(x)$ is a nonconstant polynomial.

Corollary 4.9. Let F be a field and $p(x)$ an irreducible polynomial in $F[x]$. If $p(x) \mid s_1(x)s_2(x)\cdots s_k(x)$, then $p(x)$ must divide at least one of the polynomials $s_i(x)$.

Theorem 4.10. Let F be a field. Every nonconstant polynomial is a product of irreducible polynomials in $F[x]$. This factorization is unique in the following sense. If

$$f(x) = p_1(x)\cdots p_r(x) \quad \text{and} \quad f(x) = q_1(x)\cdots q_s(x) \quad ,$$

with each $p_i(x)$ and each $q_j(x)$ irreducible, then $r = s$ and one can rearrange and relabel the factors $q_i(x)$ so that $q_i(x)$ is an associate of $p_i(x)$, $i = 1, 2, \dots, k$.

Theorem 4.11. (The Remainder Theorem). Let F be a field, $f \in F[x]$, and $a \in F$. The remainder of f when divided by the polynomial $x - a$ is $\tilde{f}(a)$ (regarded as a zero degree element of $F[x]$).

Theorem 4.12. (The Factor Theorem) Let F be a field, $f \in F[x]$, and $a \in F$. Then a is a root of the polynomial f if and only if $(x - a)$ is a factor of f in $F[x]$.

Corollary 4.13. Let F be a field and f a nonzero polynomial of degree n in $F[x]$. Then f has at most n roots in $F[x]$.

Corollary 4.14. Let F be a field and $f \in F[x]$, with $\deg(f) \geq 2$. (i) If f is irreducible in $F[x]$, then f has no roots in F . (ii) If f has degree 2 or 3 and has no roots in F , then f is irreducible in $F[x]$.

Corollary 4.15. Let F be an infinite field and $f, g \in F[x]$. Then f and g induce the same function from F to F if and only if $f = g$ in $F[x]$.