Final Exam: Friday, July 14, 2006

Show your reasoning.
Unless otherwise stated, $S$ denotes one of $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$.

1. (20 points) Using complete sentences, state the following definitions or theorems. Give formal, precise mathematical statements.

   (a) Fundamental Theorem of Arithmetic
   Every integer $n > 1$ is either a prime or a product of primes. Furthermore, the expression of $n$ as a product of primes is unique up to order.

   (b) Definition of $a$ congruent to $b$ modulo $n$
   Let $n$ be a positive integer. We say integers $a$ and $b$ are congruent modulo $n$, and write $a \equiv b \pmod{n}$, if and only if $n \mid a - b$.

   (c) Definition of root of a polynomial
   If $p(x) \in S[x]$ and $b \in S$ with $p(b) = 0$, then we say $b$ is a root of $p(x)$.

   (d) Factor Theorem
   Let $p(x) \in S[x]$ and let $r \in S$. Then $x - r \mid p(x)$ if and only if $p(r) = 0$.

   (e) Fundamental Theorem of Algebra
   If $p(x)$ is a non-constant polynomial in $\mathbb{C}[x]$, then $p(x)$ has at least one root in $\mathbb{C}$. 
2. (10 points) Indicate whether each of the following statements is true or false by circling the correct answer.

(a) True or False: If \( ac \equiv bc \pmod{n} \), then \( a \equiv b \pmod{n} \).

(b) True or False: If \( ab \equiv 0 \pmod{n} \), then \( a \equiv 0 \pmod{n} \) or \( b \equiv 0 \pmod{n} \).

(c) True or False: The degree of the zero polynomial is 0.

(d) True or False: Let \( p(x) \in \mathbb{Q}[x] \) with \( \deg p(x) > 1 \). If \( p(x) \) is reducible over \( \mathbb{Q} \), then \( p(x) \) has a root in \( \mathbb{Q} \).

(e) True or False: Let \( p(x) \in \mathbb{Q}[x] \) with \( \deg p(x) > 1 \). If \( p(x) \) has a root in \( \mathbb{Q} \), then \( p(x) \) is reducible over \( \mathbb{Q} \).

3. (4 points) Find the canonical prime factorization of the integer \( n = 18900 \).

\[
18900 = 2^2 \cdot 3^3 \cdot 5 \cdot 7
\]

4. (6 points) Let \( m = 2 \cdot 11^3 \cdot 17^5 \cdot 41 \cdot 59^2 \) and \( n = 11 \cdot 13^2 \cdot 17^3 \cdot 41^5 \cdot 59 \). Find the greatest common divisor, \( (m, n) \), and the least common multiple \( [m, n] \) of \( m \) and \( n \). Leave your answers in factored form.

(a) \( (m, n) = 11 \cdot 13^2 \cdot 17 \cdot 41 \cdot 59 \)

(b) \( [m, n] = 2 \cdot 11^3 \cdot 13^2 \cdot 17^5 \cdot 41^5 \cdot 59^2 \)

5. (5 points) Determine the number of positive divisors of the integer \( n = 10,115,600 = 2^4 \cdot 5^2 \cdot 11^3 \cdot 19 \).

\[
(4+1)(2+1)(3+1)(1+1) = 5 \cdot 3 \cdot 4 \cdot 2 = 120
\]

6. (5 points) Find \([107,602, 376,607]\) given that \(107,602, 376,607 = 53,801\) without using prime factorizations. Show your reasoning.

\[
[107,602, 376,607] = \frac{107,602 \cdot 376,607}{(107,602, 376,607)} = \frac{107,602 \cdot 376,607}{53,801} = \frac{7,632,214}{1}
\]

7. (8 points) Evaluate each of the following in the ring \( \mathbb{Z}_{12} \). Write your answers in the form \( a \) where \( a \in \{0, 1, \ldots, 11\} \). Justify your answers.

(a) \( \overline{30} \cdot (40 \cdot \overline{50}) \)

(b) \( \overline{5}^{101} \)

(c) \( \overline{-7}^{-1} \)

(d) \( \overline{7}^{-1} \)

8. (4 points) List all elements of \( \mathbb{Z}_{21} \) which have multiplicative inverses in \( \mathbb{Z}_{21} \). Write answers in the form \( a \) where \( a \in \{0, 1, \ldots, 20\} \). You do NOT have to find the multiplicative inverses of these elements.

\( \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\} \)

Note: \( a \) had a mult. inv. in \( \mathbb{Z}_{21} \) if and only if \( (a, 21) = 1 \).
9. (2 points) Evaluate: \[ \binom{10}{7} = \frac{10!}{7! \cdot 3!} = \frac{10 \cdot 9 \cdot 8 \cdot 7!}{7! \cdot 3 \cdot 2 \cdot 1} = 5 \cdot 3 \cdot 8 = 120 \]

10. (5 points) Use Pascal’s Triangle to expand \((x + 1)^6\).

\[
(x + 1)^6 = x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1
\]

11. (8 points) Use the Binomial Theorem to expand \((5x - 2)^4\).

\[
(5x - 2)^4 = \sum_{r=0}^{4} \binom{4}{r} (5x)^{4-r} (-2)^r
\]

\[
= \binom{4}{0} (5x)^4 + \binom{4}{1} (5x)^3 (-2) + \binom{4}{2} (5x)^2 (-2)^2 + \binom{4}{3} (5x) (-2)^3 + \binom{4}{4} (-2)^4
\]

\[
= 625x^4 + 4 \cdot 125 \cdot (-2)x^3 + 6 \cdot 25 \cdot 4 x^2 + 4 \cdot 5 \cdot (-8)x + 16
\]

\[
= 625x^4 - 1000x^3 + 600x^2 - 160x + 16
\]
12. (10 points) Show that each of the following is irreducible over \( \mathbb{Q} \). Justify your answers carefully.

(a) \( p(x) = x^3 + 5x^2 - 8x + 1 \)

Since \( \text{deg } p(x) = 3 \), \( p(x) \) is irreducible over \( \mathbb{Q} \) if and only if \( p(x) \) has no rational roots (Thm 3.6.6). Use Rational Roots Test: Potential rational roots: \( \pm 1 \).

\[
\begin{align*}
p(1) &= 1^3 + 5(1)^2 - 8(1) + 1 = 1 + 5 - 8 + 1 = -1 \\
 p(-1) &= (-1)^3 + 5(-1)^2 - 8(-1) + 1 = -1 + 5 + 8 + 1 = 17 \\
&\neq 0.
\end{align*}
\]

Therefore, \( p(x) \) has no roots in \( \mathbb{Q} \); since \( \text{deg } p(x) = 3 \), \( p(x) \) is irreducible over \( \mathbb{Q} \).

(b) \( p(x) = 2x^{10} + 14x^6 + 28x^5 - 42x^2 + 98x - 7 \)

Note that \( p(x) \) has all integer coefficients. Also, 7 is a prime number such that

\[
\begin{align*}
7 &\mid 42, 7 \mid 98, \text{ and } 7 \mid 7; \\
&\text{but } 7 \nmid 2 \text{ and } 7^2 \nmid 7.
\end{align*}
\]

Therefore, by Eisenstein's Criterion, \( p(x) \) is irreducible over \( \mathbb{Q} \).

13. (8 points) Find a polynomial \( p(x) \) satisfying the following conditions.

(a) \( p(x) \) has real coefficients;
(b) \( \text{deg } p(x) = 3 \);
(c) \( p(x) \) has leading coefficient 10;
(d) \( p(x) \) has 1 and \( -5i \) as roots.

Write in factored form, \( p(x) = a(x - r_1)(x - r_2) \cdots (x - r_n) \), and expanded form, \( p(x) = ax^n + a_{n-1}x^{n-1} + \cdots + a_0 \).

Since \( p(x) \) has real coefficients, \( 2 - 5i \) is a root of \( p(x) \), \( 2 + 5i \) must also be a root of \( p(x) \). Thus,

\[
\begin{align*}
p(x) &= 10(x-1)[x-(2-5i)][x-(2+5i)] \\
&= 10(x-1)[x-(2-5i)][x-(2+5i)] \\
&= 10(x-1)[x-2-5i][x-2+5i] \\
&= 10(x-1)[(x-2)^2-(5i)^2] \\
&= 10(x-1)[x^2-4x+4-25] \\
&= 10(x-1)(x^2-4x+4+29) \\
&= 10(x-1)[x^3-4x^2+29x-x^2+4x-29] \\
&= 10(x^3-5x^2+33x-29) \\
&= 10x^3-50x^2+330x-290.
\end{align*}
\]
14. (15 points) Consider the following polynomials $a(x) = 2x^3 + 8x^2 + 9x + 2$ and $b(x) = x^2 - 4$.

(a) Use the Euclidean Algorithm to find $(a(x), b(x))$, the greatest common divisor of $a(x)$ and $b(x)$. Show your reasoning.

\[
\begin{align*}
2x^3 + 8x^2 + 9x + 2 &= (2x+8)[x^2-4] + 17x + 34 \\
17x + 34 &= (\frac{17x}{17} - \frac{2}{17})[x^2 - 4] + 0
\end{align*}
\]

So $\frac{17}{17} (17x + 34) = x + 2$ is desired GCD.

↑

make it monic by clearing leading coefficient

(but note that $x + 2 \neq 17x + 34$ !)

$(a(x), b(x)) = x + 2$

(b) Use your work in the previous part to find polynomials $f(x)$ and $g(x)$ such that $(a(x), b(x)) = a(x)f(x) + b(x)g(x)$. Show your reasoning.

Solve $\boxed{17x + 34}$ for $\frac{1}{17} (17x + 34)$:

\[
\begin{align*}
17x + 34 &= [2x^3 + 8x^2 + 9x + 2] - [x^2 - 4] (2x + 8) \\
\frac{1}{17} (17x + 34) &= \frac{1}{17} \left\{ [2x^3 + 8x^2 + 9x + 2] - [x^2 - 4] (2x + 8) \right\} \\
x + 2 &= [2x^3 + 8x^2 + 9x + 2] \left(\frac{1}{17}\right) + [x^2 - 4] \left(-\frac{2}{17} x - \frac{8}{17}\right)
\end{align*}
\]

\[
\begin{align*}
f(x) &= \frac{1}{17} \\
g(x) &= -\frac{2}{17} x - \frac{8}{17}
\end{align*}
\]
15. (15 points) Let \( p(x) = 3x^4 + 9x^3 + \frac{7}{2}x^2 + 3x + 1 \).

(a) List all potential rational roots of \( p(x) \) as given by the Rational Roots Test. (Be careful here—what must you do first?) The roots of \( p(x) \) are precisely the roots of
\[
g (x) = 2p (x) = 6x^4 + 9x^3 + 7x^2 + 6x + 2.
\]
possible numerators: \( \pm 1, \pm 2 \)
possible denominators: \( \pm 1, \pm 2, \pm 3, \pm 6 \).
Possible rational roots: \( \pm 1, \pm 2, \pm \frac{1}{2}, \pm \frac{1}{3}, \pm \frac{1}{6}, \pm \frac{2}{3} \).

(b) Factor \( p(x) \) completely over \( \mathbb{C} \). (Document your methods.)
HINT: What must the sign of any real root of \( p(x) \) be? Why?

Since all coefficients of \( p(x) \) are non-negative, if \( b > 0 \),
then \( p(b) > 0 \). So all real roots of \( p(x) \) are negative.
[For convenience, we'll test the roots in \( g(x) \), factor \( g(x) \), then find factored form of \( p(x) \).]

\[
\begin{align*}
\frac{-1}{1} & | 6 & 9 & 4 & 6 & 2 \\
-1 & | -6 & -3 & -4 & -2 & 0 \\
\frac{6}{6} & 3 & 4 & 2 & 10 & 0 & \checkmark
\end{align*}
\]

\[
\begin{align*}
-1 & | 6 & 3 & 4 & 2 & 0 \\
-1 & | -6 & +3 & -1 & 0 \\
\frac{6}{6} & -3 & 7 & -5 & 0 & \checkmark
\end{align*}
\]

\[
\begin{align*}
\text{So } g(x) &= (x+1)(6x^3 + 3x^2 + 4x + 2) \\
\frac{-1}{2} & | 6 & 3 & 4 & 2 \\
-1 & | -12 & 18 & -44 & 0 \\
\frac{6}{6} & -9 & 22 & -42 & 0 & \checkmark
\end{align*}
\]

\[
\begin{align*}
\text{So } g(x) &= (x+1)(x + \frac{1}{2})(6x^2 + 4) \\
&= 6(x+1)(x + \frac{1}{2})(x^2 + \frac{2}{3}) \\
&= 6(x+1)(x + \frac{1}{2})[x + \sqrt{\frac{2}{3}} i][x - \sqrt{-\frac{2}{3}} i]
\end{align*}
\]

Thus, \( p(x) = \frac{1}{2} g(x) \)
\[
= 3 (x+1)(x + \frac{1}{2})(x + \sqrt{\frac{2}{3}} i)(x - \sqrt{\frac{2}{3}} i) \]
16. (10 points) Using the definition of \( \mathbb{Z}_n \) (including the definition of multiplication in \( \mathbb{Z}_n \)) and the algebraic properties of the ring \( \mathbb{Z} \) of integers, prove that multiplication in \( \mathbb{Z}_n \) is associative. That is, if \( a, b, c \in \mathbb{Z}_n \), then \( a \cdot (b \cdot c) = (a \cdot b) \cdot c \). Indicate clearly where the properties of \( \mathbb{Z} \) are being used.

\[
\begin{align*}
\text{Proof. } \text{Let } \bar{a} & \in \mathbb{Z}^+ \text{ and suppose } \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n. \text{ Then } \\
\bar{a} \cdot (\bar{b} \cdot \bar{c}) &= \bar{a} \cdot \bar{bc} & \text{(by defn of } \cdot \text{ in } \mathbb{Z}_n) \\
&= \bar{a} \cdot \bar{bc} & \text{(by defn of } \cdot \text{ in } \mathbb{Z}_n) \\
&= \bar{a} \cdot \bar{bc} & \text{(by associativity of } \cdot \text{ in } \mathbb{Z}) & \star \\
&= \bar{a} \cdot \bar{bc} & \text{(by defn of } \cdot \text{ in } \mathbb{Z}_n) \\
&= (\bar{a} \cdot \bar{b}) \cdot \bar{c} & \text{(by defn of } \cdot \text{ in } \mathbb{Z}_n). \\
\end{align*}
\]

Hence, multiplication in \( \mathbb{Z}_n \) is associative. \( \blacksquare \)

17. (10 points) Using the definition of \( \mathbb{R}[x] \) (including the definition of addition in \( \mathbb{R}[x] \)) and the algebraic properties of the field \( \mathbb{R} \) of real numbers, prove that polynomial addition in \( \mathbb{R}[x] \) is commutative. That is, if \( a(x), b(x) \in \mathbb{R}[x] \), then \( a(x) + b(x) = b(x) + a(x) \). Indicate clearly where the properties of \( \mathbb{R} \) are being used.

\[
\begin{align*}
\text{Proof. } \text{Let } a(x), b(x) & \in \mathbb{R}. \text{ Write } a(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \\
& \quad \text{and } b(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0. \text{ Then } \\
a(x) + b(x) &= (a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) + (b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0) \\
&= (a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) + (b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0) \\
&= (a_n + b_n) x^n + (a_{n-1} + b_{n-1}) x^{n-1} + \cdots + (a_1 + b_1) x + (a_0 + b_0) & \text{(by defn of } + \text{ in } \mathbb{R}[x]) \\
&= (b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0) + (a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) & \text{(by commutativity of } + \text{ in } \mathbb{R}) & \star \\
&= b(x) + a(x). \\
\end{align*}
\]

Therefore, addition in \( \mathbb{R}[x] \) is commutative. \( \blacksquare \)
18. (10 points) Prove that congruence modulo \( n \) is transitive. That is, if \( a, b, c \in \mathbb{Z} \) with \( a \equiv b \) (mod \( n \)) and \( b \equiv c \) (mod \( n \)), then \( a \equiv c \) (mod \( n \)).

**Proof.** Let \( n \in \mathbb{Z}^+ \). Suppose \( a, b, c \in \mathbb{Z} \) such that \( a \equiv b \) (mod \( n \)) and \( b \equiv c \) (mod \( n \)). This means \( n \mid a-b \) and \( n \mid b-c \).

Now \[
\begin{align*}
a - c &= a - b + b - c \\
&= (a - b) + (b - c).
\end{align*}
\]

Since \( n \mid a-b \) and \( n \mid b-c \), by the Combination Theorem, \( n \mid a-c \). That is, \( a \equiv c \) (mod \( n \)). Therefore, congruence modulo \( n \) is transitive. \[\qed \]

19. (10 points) Prove that "divides" in \( S[x] \) is transitive. That is, if \( a(x), b(x), c(x) \in S[x] \) with \( a(x) \mid b(x) \) and \( b(x) \mid c(x) \), then \( a(x) \mid c(x) \).

**Proof.** Let \( a(x), b(x), c(x) \in S[x] \) such that \( a(x) \mid b(x) \) and \( b(x) \mid c(x) \). Then there exist polynomials \( r(x), s(x) \in S[x] \) such that \( b(x) = a(x)r(x) \) and \( c(x) = b(x)s(x) \).

Thus,
\[
\begin{align*}
c(x) &= b(x)s(x) \\
&= (a(x)r(x))s(x) \\
&= a(x)(r(x)s(x)).
\end{align*}
\]

This shows that \( a(x) \mid c(x) \). Therefore, "divides" in \( S[x] \) is transitive. \[\qed \]