NAME: (print!) [Signature]

E-Mail address: [Email address]

MATH 356, Dr. Z., Final Exam, Mon., Dec. 23, 2013, 8-11am, SEC-218

Do not write below this line (office use only)

1. [Score] (out of 10)
2. [Score] (out of 10)
3. [Score] (out of 10)
4. [Score] (out of 10)
5. [Score] (out of 10)
6. [Score] (out of 10)
7. [Score] (out of 10)
8. [Score] (out of 10)
9. [Score] (out of 10)
10. [Score] (out of 10)
11. [Score] (out of 10)
12. [Score] (out of 10)
13. [Score] (out of 10)
14. [Score] (out of 10)
15. [Score] (out of 10)
16. [Score] (out of 10)
17. [Score] (out of 10)
18. [Score] (out of 10)
19. [Score] (out of 10)
20. [Score] (out of 10)

tot.: [Score] (out of 200)
1. Using the formula (no credit for other methods!), find the unique $x$ between 0 and 98 such that

$$x \equiv 7 \pmod{9}, \quad x \equiv 6 \pmod{11}.$$

**Reminder:** The unique solution of the system $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}$ in $0 \leq x < m_1m_2$, when $m_1$ and $m_2$ are relatively prime

$$x \equiv a_1m_2[m_2^{-1}]_{m_1} + a_2m_1[m_1^{-1}]_{m_2} \pmod{m_1m_2}.$$

(Note: you may find the modular inverse by trial-and-error rather than by the 'official' way, using the Extended Euclidean Algorithm.)

**Ans.:** $x = 61$

\[
\begin{align*}
9_1 &= 7 & a_2 &= 6 \\
m_1 &= 9 & m_2 &= 11 \\
[m_1^{-1}]_{m_2} &= \left[9^{-1}\right]_m = 5 & [m_2^{-1}]_{m_1} &= \left[11^{-1}\right]_m = 5 \\
[9 \cdot 5]_m &= \left[45\right]_m = 1 & [11 \cdot 5]_m &= \left[55\right]_m = 1 \\
\end{align*}
\]

\[
\begin{align*}
x &= \left(7 \cdot 11 \cdot 5 + 6 \cdot 9 \cdot 5\right) \pmod{99} \\
&= \left(377 + 270\right) \pmod{99} \\
&= \left(647\right) \pmod{99} \\
&= 61 \\
\end{align*}
\]

\[
\begin{align*}
[61]_9 &= 7 \\
[61]_{11} &= 4
\end{align*}
\]
2. (10 pts.) Prove that if you take any 3-digit positive integer written in decimal positional notation (as usual!)

\[ i_2 i_1 i_0 \ , \ (1 \leq i_2 \leq 9 \ , \ 0 \leq i_1 \leq 9 \ , \ 0 \leq i_0 \leq 9 ) \]

then the 6-digit decimal integer obtained by repeating it (for example, if you take 395 you make 395395), namely

\[ i_2 i_1 i_0 i_2 i_1 i_0 \ , \]

is divisible by 13.

The divisibility test is if the alternating sum of every 3 digits is divisible by 13 (or \( \text{mod} \ 13 \)) then the number is divisible by 13.

\[ i_2 i_1 i_0 - i_2 i_1 i_0 = 0 \]

The alternating sum will be \( i_2 i_1 i_0 - i_2 i_1 i_0 = 0 \)

The alternating sum is \( \text{O mod} \ 13 = \Rightarrow 13 \mid i_2 i_1 i_0 i_2 i_1 i_0 \)

**Correct, but here is a proof from scratch:**

\[ i_2 i_1 i_0 i_2 i_1 i_0 = i_2 \cdot 10^5 + i_1 \cdot 10^4 + i_0 \cdot 10^3 + i_2 \cdot 10^2 + i_1 \cdot 10 + i_0 \]

\[ = 10^3 \left( i_2 \cdot 10^2 + i_1 \cdot 10 + i_0 \right) + 1 \cdot \left( i_2 \cdot 10^2 + i_1 \cdot 10 + i_0 \right) \]

\[ = 1001 \cdot \left( i_2 \cdot 10^2 + i_1 \cdot 10 + i_0 \right) = 13 \cdot 71 \left( i_2 \cdot 10^2 + i_1 \cdot 10 + i_0 \right) \]

$$(p-1)! = -1 \pmod{p}$$

$$(13-1)! = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$$

If we pair the numbers with their multiplicative inverses $\pmod{13}$

\[
\begin{align*}
[2 \cdot 6]_{13} &= 1 \\
[3 \cdot 9]_{13} &= 1 \\
[5 \cdot 8]_{13} &= 1 \\
[10 \cdot 4]_{13} &= 1 \\
[7 \cdot 11]_{13} &= 1
\end{align*}
\]

\[
= (2 \cdot 0)(3 \cdot 9)(5 \cdot 8)(10 \cdot 4)(7 \cdot 11)(1 \cdot 2) \pmod{13}
\]

\[
= \mathcal{A} \quad 12 \mod{13} = -1 \pmod{13}
\]
4. (10 pts.) Use the Fermat primality test to investigate whether 13 is prime or composite by picking two random a's between 2 and 12.

If \( a^{p-1} \equiv 1 \pmod{p} \) then p is probably prime.

my random a: \( a = 2 \):

\[
\begin{align*}
2^2 &\equiv 2 \\
2^4 &\equiv 4 \\
2^6 &\equiv 3 \\
2^8 &\equiv 9 \\
2^{12} &\equiv 1 \pmod{13} \quad \checkmark \\
\end{align*}
\]

\( a^2 = 2 \) is a witness to p's primality.

a = 3

\[
\begin{align*}
3^2 &\equiv 3 \\
3^4 &\equiv 9 \\
3^6 &\equiv 3 \\
3^8 &\equiv 9 \\
3^{12} &\equiv 1 \pmod{13} \quad \checkmark
\end{align*}
\]

3 is a witness to p's primality.
5. (10 pts.) Compute $\phi(18000)$ . Explain!

Ans.: $\phi(18000) = 4800$

Prime decomposition of 18000:

$10 \cdot 1800$
$10 \cdot 180$
$10 \cdot 10 \cdot 18$
$2^3 \cdot 5^3 \cdot 18$
$2^4 \cdot 5^3 \cdot 9$

$18000 = 2^4 \cdot 3^2 \cdot 5^3$

The number of integers $x$

$1 \leq x \leq n-1$ relatively prime to $n$

$\gcd(x,n) = 1.$

$\phi(18000) = 18000 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right)$

$= 18000 \left(\frac{1}{2}\right) \left(\frac{2}{3}\right) \left(\frac{4}{5}\right)$

$= 2^4 \cdot 3 \cdot 5^2 \cdot 4 = 4800$

$2 \div 4$

$\frac{1}{6} \div 4$

$\frac{1}{6} \div 3$

$\frac{2}{19} \div 2$

$\frac{2}{19} \div 25$

$1940$

$3440$

$4800$
6. (10 pts.) Suppose Alice used RSA to send you the encrypted message $c$, using the public key $e$ that you gave her. Check that this is an OK message (coprime to $n = pq$). Also check that the key is a valid key. If they are both OK, find her original message, $m$.

$$p = 11, \quad q = 13, \quad e = 7, \quad c = 3.$$ 

\[\sqrt{10}\]

Ans.: $m = 16$

i) $n = p \cdot q = 11 \times 13 = 143$

\[\phi(n) = \phi(143) = 143 \times \left(1 - \frac{1}{11}\right) \left(1 - \frac{1}{13}\right) = 10 \times 12 = 120\]

\[\gcd(e, \phi(n)) = \gcd(7, 120) = \gcd(120, 7) = 7, \quad \text{so } e \text{ is OK.}\]

ii) $d = e^{-1} \mod \phi(n) = 7^{-1} \mod 120 = -17 + 120 = 103$

(Since $1 = 120 - 11 \times 7$)

iii) $\gcd(c, n) = \gcd(3, 143) = \gcd(143, 3) = 1, \quad \text{so } c \text{ is OK.}\]

iv) $m = c^d \mod n = 3^{103} \mod 143 = 3^{3^4 \cdot 3^2 \cdot 3^1 \cdot 3^0} \mod 143$

\[3^1 \mod 143 = 3\]

\[3^2 \mod 143 = 9\]

\[3^3 \mod 143 = -62\]

\[3^4 \mod 143 = -17\]

\[3^6 \mod 143 = 2\]

\[3^{32} \mod 143 = 9\]

\[3^{34} \mod 143 = -62\]

\[= (-62) \cdot 9 \cdot (-62) \cdot 9 \cdot 3 \mod 143\]

\[= (-17) \cdot (-62) \cdot 3 \mod 143\]

\[= 16\]
7. (10 pts.) Prove that for every positive integer \( n \), the number of partitions of \( n \) into odd parts equals the number of partitions of \( n \) with distinct parts.

\[
\text{distinct}(n) = \frac{1}{1 - q^{2n-1}} (1 + q^n)
\]

\[
\text{odd}(n) = \frac{1}{\prod_{i=1}^{k} (1 - q^{2i-1})}
\]

\[
\prod_{i=1}^{k} (1 + q^i) = (1 + q) (1 + q^2) (1 + q^3) \ldots
\]

generating

\[
= \left( \frac{1 - q^2}{1 - q} \right) \left( \frac{1 - q^4}{1 - q^2} \right) \left( \frac{1 - q^6}{1 - q^3} \right) \left( \frac{1 - q^8}{1 - q^4} \right) \left( \frac{1 - q^{10}}{1 - q^5} \right)
\]

Only even powers of \( q \) appear in the numerator because they are of the form \( 2i \).

They cancel with all of the even denominators

\[
\left( \frac{1 - q^2}{1 - q} \right) \left( \frac{1 - q^4}{1 - q^2} \right) \left( \frac{1 - q^6}{1 - q^3} \right) \left( \frac{1 - q^8}{1 - q^4} \right) \left( \frac{1 - q^{10}}{1 - q^5} \right) = \left( \frac{1}{1 - q} \right) \left( \frac{1}{1 - q^2} \right) \left( \frac{1}{1 - q^3} \right)
\]

Thus, they are equal

\[
\frac{z + 1}{1 - z} = \frac{1 - z^2}{1 - z}
\]

\[
1 + z = \frac{1 - z^2}{1 - z}
\]
8. (10 pts.) Prove that if $p$ is prime, and $2^p - 1$ is also prime, then $n = 2^{p-1}(2^p - 1)$ is a perfect number.

*perfect number*

\[ n = 2^{p-1}(2^p - 1) \]

*6(n) = 2n.*

 فلاً

\[ 6(n) = (1 + p + p^2 + \ldots + p^{\alpha - 1}) \cdot (1 + p + \ldots + p^{\delta - 1}) \]

\[ = 2^p \left( 1 + 2 + \ldots + 2^{p-1} \right) \]

\[ = 2^p \left( 2^p - 1 \right) \]

\[ = 2 \left[ 2^{p-1}(2^p - 1) \right] = 2n \]

\[ \sqrt{10} \]
9. (10 pts.) What is \( \mu(2002) \)? (\( \mu(n) \) is the famous Möbius function). Explain!

\[ \text{Ans.: } \mu(2002) = 1 \]

So if prime decomposition has a square,
\[ \mu(n) = (-1)^k \text{ where } k \text{ is # of primes in the decomposition}. \]

\[ 2002 = 2 \cdot 1001 = 2 \cdot 7 \cdot 11 \cdot 13 \]

2002 is square free so \( \mu(2002) \neq 0 \).

\[ k = 4 \text{ because } |\{2, 7, 11, 13\}| = 4 \]

\[ (-1)^4 = 1 \]
10. (10 pts.) Using the four rules below (most famously the Quadratic Reciprocity Law) decide whether 17 is a quadratic residue modulo 101. Explain everything.

Ans.: 17 \( \bigcirc \) is not a quadratic residue mod 101.

Rule 1: If \( p \) is an odd prime and \( a \) and \( b \) are not multiples of \( p \), then
\[
\left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right)
\]

Rule 2: If \( p \) is an odd prime then
\[
\left( \frac{-1}{p} \right) = (-1)^{(p-1)/2}
\]

Rule 3: If \( p \) is an odd prime then
\[
\left( \frac{2}{p} \right) = (-1)^{(p^2-1)/8}
\]

Rule 4: (The quadratic Reciprocity Law)
If \( p \) and \( q \) are distinct odd primes, then
\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{(p-1)(q-1)/4}
\]

\[
\left( \frac{17}{101} \right) \left( \frac{101}{17} \right) = (-1)^{17 \cdot 101 / 4} = 1 \quad \Rightarrow \quad \left( \frac{17}{101} \right) = \left( \frac{101}{17} \right)
\]

\[
\left( \frac{101}{17} \right) = \left( \frac{-1}{17} \right) = (-1)^{17/2} = (-1)^9 = 1
\]

Therefore, 101 \( \equiv -1 \pmod{17} \)

\[
\left( \frac{-1}{17} \right) = \left( \frac{101}{17} \right) = \left( \frac{17}{101} \right) = 1 \quad \Rightarrow \quad 17 \text{ is a quadratic residue of } 101.
\]
11. (10 pts) Apply the famous Bressoud-Zeilberger map to the pair
\[ \lambda = (7, 5, 3, 2, 2, 1, 1, 1) \quad , \quad j = 2 \]

Call the output \((\lambda', j')\). Then apply it to the output, and show that you get \((\lambda, j)\) back.

\[
\text{Ans.:} \quad \lambda' = (14, 4, 4, 2, 1, 1, 1) \quad \text{and} \quad j' = 1
\]

\[ \textbf{Reminder:} \quad \text{Let} \quad \lambda = (\lambda(1), \ldots, \lambda(t)) \quad \text{where} \quad t \quad \text{is the number of parts.} \quad \text{If} \quad t + 3j \geq \lambda(1) \quad \text{then} \]
\[ \lambda' = (t + 3j - 1, \lambda(1) - 1, \ldots, \lambda(t) - 1) \quad \text{if erasing all zeros at the end, of course, and} \quad j' = j - 1. \]
\[ \text{Otherwise} \quad \lambda' = (\lambda(2) + 1, \ldots, \lambda(t) + 1, \lambda(1) - 3j - 1), \text{and} \quad j' = j + 1. \]

\[ \psi(\lambda) = \psi (7, 5, 3, 2, 2, 2, 1, 1) \quad \text{and} \quad j = 2 \]
\[ t = 9 \quad \quad \quad \quad \quad \quad \quad \quad \text{and:} \quad t + 3j = 9 + 6 = 15 \geq \lambda = 7 \]
\[ \lambda, = 7 \]
\[ \lambda' = (14, 4, 4, 2, 1, 1, 1) \quad \text{and} \quad j' = j - 1 = 2 - 1 = 1 \]

\[ \psi(\lambda') = \psi(\lambda') = \psi (14, 4, 4, 2, 1, 1, 1) \]
\[ \lambda' = 14 \quad \quad \quad \text{and} \quad t' = 7 \]
\[ t' + 3j' = 7 + 3 = 10 < 14 = \lambda' \]

\[ \lambda = \lambda'' = (14, 7, 3, 2, 2, 2, 1, 1, 1) \quad \text{and} \quad j'' = 0 \]

\[ \textbf{Number of Ones:} \quad \lambda, - 3j - t - 1 = 14 - 7 - 3 - 1 = 10 - 11 = 3 \]
12. (10 pts.) Apply Franklin's bijection to the distinct partition $\lambda = (15, 14, 13, 12, 6, 5, 2)$, if it is applicable. If it is indeed applicable, call the output $\lambda'$, and apply Franklin's bijection to $\lambda'$ and show that you get $\lambda$ back.

Ans.: $\lambda' = (14, 15, 13, 12, 4, 5, 2)$
13. (10 pts.) Let $n$ and $k$ be positive integers, with $k \leq n$. Prove that the number of partitions of $n$ with exactly $k$ parts equals the number of partitions of $n$ whose largest part is $k$.

For every partition $\lambda$, there is a $\lambda'$ calculable from the Ferrer diagram of the partition illustrating this bijection.

Let $n = 30$

$k = 5$

Partitions of 30 with $k$ parts example

$\lambda = (8, 7, 6, 5, 4)$

Take $\lambda'$ to be the columns of the Ferrer diagram of $\lambda$, so for $\lambda'$ = $5, 5, 5, 5, 4, 3, 2, 1$ this is also a partition of $n = 30$

Apply the same map to get back

Thus, number of partitions of $n$ with $k$ parts equals number of partitions of $n$ whose largest part is $k$. 

$\lambda'' = \lambda = (8, 7, 6, 5, 4)$
14. (10 pts.) Convert \( \frac{37}{88} \) into a simple continued fraction.

Ans.: \( \frac{37}{88} = \frac{1}{1 + \frac{1}{2 + \frac{1}{18}}} \)

\[
\text{CF} \left( \frac{37}{88} \right) = 0 + \frac{1}{\text{CF} \left( \frac{55}{34} \right)} = 0 + \frac{1}{1 + \frac{1}{2 + \frac{1}{18}}}
\]

\[
\text{CF} \left( \frac{55}{34} \right) = 1 + \frac{1}{\text{CF} \left( \frac{21}{18} \right)} = 1 + \frac{1}{2 + \frac{1}{18}}
\]

\[
\text{CF} \left( \frac{21}{18} \right) = 2 + \frac{1}{\text{CF} \left( \frac{3}{18} \right)} = 2 + \frac{1}{18}
\]
15. (10 pts.) Evaluate the infinite continued fraction \( x = [5, 1, 3, 1, 1, 1, 3, 1, 3, 1, 3, \ldots] \) (i.e. \( x = [5, (1, 3)^\infty] \) that starts with 5 followed by 1, 3 repeated an infinite number of times) as a quadratic irrationality.

Ans.: \( x = \frac{7 + \sqrt{21}}{2} \)
16. (10 pts.) In Planet Z there are 9 days in the week, and the year-length is always the same (no leap years!), consisting of 400 days. If today is 3-Day, what day of the week would it be (on planet Z) at the same date as today, but exactly 1000 years later? Explain!

Ans.: It would be 7-Day.

\[ 400 \mod 9 \to \text{calculate how much the day changes each year} \]
\[ = 4 \implies +4 \text{ to the day of the week for every year} \]
\[ 3 + (1000 \times 4) \mod 9 \equiv 3 + 4 \mod 9 = 7 \]
17. (10 pts.) Using the Extended Euclidean algorithm (no credit for other methods!), find out whether it is possible to express 1 as a linear combination

\[ 1 = m \cdot 23 + n \cdot 97, \]

for some integers \( m \) and \( n \), and if it is possible, find \( m \) and \( n \).

Ans.: \( m = 38 \), \( n = -9 \).

\[
\gcd(97, 23) = \gcd(23, 5) = \gcd(5, 3) = \gcd(3, 2) = \gcd(2, 1) = 1
\]

\[ \Rightarrow \text{ linear combination possible!!} \]

\[
97 = 23 \cdot 4 + 5 \\
23 = 5 \cdot 4 + 3 \\
5 = 3 \cdot 1 + 2 \\
3 = 2 \cdot 1 + 1
\]

\[
97 = 4 \cdot 23 + 5 \\
23 = 4 \cdot 5 + 3 \\
5 = 3 \cdot 1 + 2 \\
3 = 2 \cdot 1 + 1
\]

\[
5 = \underbrace{97 - 4 \cdot 23} \\
= \underbrace{23 - 4(123 - 4 \cdot 23)} \\
= 23 - 4 \cdot 123 + 16 \cdot 23
\]

\[
3 = \underbrace{23 - 4 \cdot 5} \\
= \underbrace{23 - 4(3 \cdot 5 + 1 \cdot 23)} \\
= 23 - 4 \cdot 15 + 4 \cdot 23
\]

\[
2 = 5 - 3 = \underbrace{97 - 4 \cdot 23} \\
= \underbrace{23 - 4 \cdot 123} + 4 \cdot 97
\]

\[
1 = 3 - 2 = \underbrace{97 - 4 \cdot 23} - 5 \cdot 97 + 21 \cdot 23
\]

\[
1 = 38 \underbrace{23} - 9 \underbrace{97}
\]
18. (10 pts.) Express the integer 487 (written in our usual (base 10) notation) in base 7, in (i) sparse notation (4 pts) (ii) dense notation (3 pts) (iii) base-seven positional notation (3 pts)

**Ans.:**
(i) $1 \cdot 7^3 + 2 \cdot 7^2 + 6 \cdot 7^1 + 4 \cdot 7^0$
(ii) $1 \cdot 7^3 + 2 \cdot 7^2 + 6 \cdot 7^1 + 4 \cdot 7^0$
(iii) $12404$

487 base 10 $\rightarrow$ base 7

1. $1 \cdot 7^3 + 2 \cdot 7^2 + 6 \cdot 7^1 + 4 \cdot 7^0$  
   $\checkmark$  

2. 49  
   42  
   4  
   $= 98$

---

### (ii) dense is sparse because there are no powers of 7 with zero coefficients.
19. (10 pts.) Let $T_n$ be the Tribonacci numbers, defined by

$$T_1 = 1, \quad T_2 = 1, \quad T_3 = 1,$$

and for $n \geq 4$,

$$T_n = T_{n-1} + T_{n-2} + T_{n-3}.$$ 

Give a Zeilberger-style proof of the following identity,

$$T_{n+2} = 4T_{n-1} + 3T_{n-2} + 2T_{n-3},$$

by checking it empirically for $n = 4, 5, 6, 7$.

$n = 4$:

$$T_6 = 4T_3 + 3T_2 + 2T_1$$

$$9 = 4(1) + 3(1) + 2(1) = 9 \quad \checkmark$$

$n = 5$:

$$T_7 = 4T_4 + 3T_3 + 2T_2$$

$$17 = 4(3) + 3(1) + 2(1) = 12 + 3 + 2 = 17 \quad \checkmark$$

$n = 6$:

$$T_8 = 4T_5 + 3T_4 + 2T_3$$

$$31 = 4(5) + 3(3) + 2(1) = 20 + 9 + 2 = 31 \quad \checkmark$$

$n = 7$:

$$T_9 = 4T_6 + 3T_5 + 2T_4$$

$$57 = 4(9) + 3(5) + 2(3) = 36 + 15 + 6 = 57 \quad \checkmark$$

$\checkmark \quad 10$
20. (10 pts.) Use the Fundamental Theorem of Discrete Calculus to prove the identity

\[ \sum_{i=1}^{n} i(i+1)(i+2) = \frac{1}{4} n(n+1)(n+2)(n+3). \]

**Proof:**

\[ a(i) = i(i+1)(i+2), \quad s(n) = \frac{1}{4} n(n+1)(n+2)(n+3). \]

\[ s(0) = \frac{1}{4} \cdot 0 \cdot (0+1)(0+2)(0+3) = 0. \]

\[ s(n) - s(n-1) = \frac{1}{4} n(n+1)(n+2)(n+3) - \frac{1}{4} (n-1)(n-1+1)(n-1+2)(n-1+3). \]

\[ = \frac{1}{4} n(n+1)(n+2)(n+3) - \frac{1}{4} (n-1)(n)(n+1)(n+2). \]

\[ = \frac{1}{4} n(n+1)(n+2) \left[ n+3 - (n-1) \right]. \]

\[ = \frac{1}{4} n(n+1)(n+2) \cdot 4. \]

\[ = n(n+1)(n+2) = a(n). \]

Thus

\[ \sum_{i=1}^{n} i(i+1)(i+2) = \frac{1}{4} n(n+1)(n+2)(n+3). \]

\[ \boxed{10} \]