SOLUTIONS TO PROBLEM SET 3

1. Section 6.1

Problem 4. We want to find $r \in \mathbb{Z}$ such that
\[ 5!25! \equiv r \pmod{31} \quad \text{and} \quad 0 \leq r \leq 30. \]
By Wilson’s theorem $30! \equiv -1 \pmod{31}$. Then,
\[ 5!25! \equiv 25! \cdot (-26) \cdot (-27) \cdot (-28) \cdot (-29) \cdot (-30) \equiv (-1)^2 \cdot 30! \equiv (-1)^6 \equiv 1 \pmod{31}, \]
that is $r = 1$.

Problem 10. We want to find $r \in \mathbb{Z}$ such that
\[ 6^{2000} \equiv r \pmod{11} \quad \text{and} \quad 0 \leq r \leq 10. \]
Since 11 is prime and $(6, 11) = 1$ by Fermat’s little theorem we have $6^{10} \equiv 1 \pmod{11}$. Then,
\[ 6^{2000} = (6^{10})^{200} \equiv 1^{200} \equiv 1 \pmod{11}, \]
thus $r = 1$.

Problem 12. We want to find $r \in \mathbb{Z}$ such that
\[ 2^{1000000} \equiv r \pmod{17} \quad \text{and} \quad 0 \leq r \leq 16. \]
Since 17 is prime and $(2, 17) = 1$ by FLT we have $2^{16} \equiv 1 \pmod{17}$. Then,
\[ 2^{1000000} = (2^{16})^{625} \equiv 1 \pmod{17}, \]
thus $r = 1$.

Problem 24. It is a corollary of FLT that $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$. Then
\[ 1^p + 2^p + 3^p + \ldots + (p-1)^p \equiv 1 + 2 + 3 + \ldots + (p-1) \pmod{p}. \]
Note that since $p$ is odd $p-1$ is even and
\[ p - \frac{p-1}{2} = \frac{2p-1}{2} = \frac{p+1}{2}. \]
Moreover, we can rearrange the sum above as the following sum of $(p-1)/2$ terms
\[ 1 + 2 + 3 + \ldots + (p-1) \equiv (1 + (p-1)) + (2 + (p-2)) + \ldots + \left( \frac{p-1}{2} + \frac{p+1}{2} \right) \pmod{p} \]
\[ \equiv p + p + \ldots p \equiv 0 \pmod{p}. \]

Date: October 19, 2016.
Problem 26. Let \( r_k \equiv 2^{k!} \pmod{689} \) for \( k \in \mathbb{Z}_{>0} \). We have \( r_{k+1} \equiv r_k^{k+1} \pmod{689} \). We successively compute \( r_k \) and \( (r_k - 1, 689) \) until the latter is different from 1, in which case we have found a divisor of 689. Indeed,

\[
\begin{align*}
  r_1 &= 2^1 \equiv 2 \pmod{689} \\
  r_2 &= 2^2 \equiv 4 \pmod{689} \\
  r_3 &= 4^3 \equiv 64 \pmod{689} \\
  r_4 &= 64^4 \equiv 4096^2 \equiv 651^2 \equiv 423801 \equiv 66 \pmod{689}
\end{align*}
\]

and respectively

\[
(1, 689) = 1, \quad (3, 689) = 1, \quad (63, 689) = 1, \quad (65, 689) = 13.
\]

Thus \( 13 \mid 689 \).

2. Section 6.2

Problem 2. Note that \( 45 = 9 \cdot 5 \) is composite and \( (17, 45) = (19, 45) = 1 \).

We have

\[
17^4 \equiv 2^4 \equiv 16 \equiv 1 \pmod{5} \quad \text{and} \quad 17^4 \equiv (-1)^4 \equiv 1 \pmod{9}.
\]

Since \( (5, 9) = 1 \) the CRT implies that \( 17^4 \equiv 1 \pmod{45} \), therefore

\[
17^{44} = (17^4)^{11} \equiv 1 \pmod{45}
\]

and we conclude 45 is a pseudoprime for the base 17.

We have

\[
19^2 \equiv (-1)^2 \equiv 1 \pmod{5} \quad \text{and} \quad 19^2 \equiv 1^2 \equiv 1 \pmod{9}.
\]

Since \( (5, 9) = 1 \) the CRT implies that \( 19^2 \equiv 1 \pmod{45} \), therefore

\[
19^{44} = (19^2)^{22} \equiv 1 \pmod{45}
\]

and we conclude 45 is a pseudoprime for the base 19.

Problem 8. Let \( p \) be prime and write \( N = 2^p - 1 \).

Suppose \( N \) is composite; hence \( p \geq 3 \). Since \( (2, p) = 1 \) we have \( 2^{p-1} \equiv 1 \pmod{p} \) by FLT and so \( 2^{p-1} - 1 = pk \) for some odd \( k \in \mathbb{Z} \). Thus

\[
N - 1 = 2^p - 2 = 2(2^{p-1} - 1) = 2pk.
\]

Note also that \( 2^p \equiv N + 1 \equiv 1 \pmod{N} \); thus

\[
2^{N-1} = 2^{2pk} = (2^p)^{2k} \equiv 1 \pmod{N},
\]

that is \( N \) is a pseudoprime to the base 2.
Problem 12. An odd composite \( N > 0 \) is a strong pseudoprime for the base \( b \) if it fools Miller’s Test in base \( b \). Recall that to be possible to apply the \((k+1)\)-th step of Miller’s test in base \( b \) we need
\[
b^{(N-1)/2^k} \equiv 1 \pmod{N} \quad \text{and} \quad N - 1 \text{ is divisible by } 2^{k+1}.
\]
Let \( N = 25 \). We have \( N - 1 = 25 - 1 = 24 = 2^3 \cdot 3 \). We first observe that
\[
7^6 = (7^2)^3 \equiv 49^3 \equiv (-1)^3 \equiv -1 \pmod{25}.
\]
We now apply Miller’s test
\[
7^{24} \equiv (7^6)^4 \equiv (-1)^4 \equiv 1 \pmod{25} \quad \text{(i.e. 25 is a pseudoprime to base 7)},
\]
\[
7^{12} \equiv (7^6)^2 \equiv (-1)^2 \equiv 1 \pmod{25},
\]
\[
7^6 \equiv -1 \pmod{25};
\]
despite the fact that 6 is divisible by 2 the last congruence means we have to stop.
Therefore 25 fools the test, i.e. it is a strong pseudoprime to the base 7.

Problem 18.

a) Let \( m \in \mathbb{Z}_{>0} \) be such that \( 6m + 1, 12m + 1 \) and \( 18m + 1 \) are prime numbers. Write \( n = (6m + 1)(12m + 1)(18m + 1) \) and let \( b \in \mathbb{Z}_{>2} \) satisfy \((b, n) = 1\).
As \( 6m + 1 \mid n \) we also have \((6m + 1, b) = 1\) hence \( b^{6m} \equiv 1 \pmod{6m + 1} \) by FLT. Similarly, we conclude also that
\[
b^{12m} \equiv 1 \pmod{12m + 1} \quad \text{and} \quad b^{18m} \equiv 1 \pmod{18m + 1}.
\]
Now note that
\[
n = 6 \cdot 12 \cdot 18m^3 + (6 \cdot 12 + 6 \cdot 18 + 12 \cdot 18)m^2 + 36m + 1
\]
then \(6m \mid n - 1, 12m \mid n - 1\) and \(18m \mid n - 1\). Thus the following congruence hold
\[
b^{n-1} \equiv 1 \pmod{6m + 1}
\]
\[
b^{n-1} \equiv 1 \pmod{12m + 1}
\]
\[
b^{n-1} \equiv 1 \pmod{18m + 1}
\]
and since \(6m + 1, 12m + 1\) and \(18m + 1\) are pairwise coprime (because they are distinct primes) by CRT we conclude that \( b^{n-1} \equiv 1 \pmod{n} \). Since \( b \) was arbitrary we conclude that \( n \) is a Carmichael number.

b) Take respectively \( m = 1, 6, 35, 45, 51 \).

3. Section 6.3

Problem 6. The question is equivalent to find \( r \in \mathbb{Z} \) such that
\[
7^{999999} \equiv r \pmod{10} \quad \text{and} \quad 0 \leq r \leq 9.
\]
Since \((7, 10) = 1\) and \(\phi(10) = 4\) then \(7^4 \equiv 1 \pmod{10}\) by Euler’s theorem.
Note that \(999996 = 4 \cdot 249999\), then
\[
7^{999999} = 7^{999996} \cdot 7^3 = (7^4)^{249999} \cdot 7^3 \equiv 1 \cdot 7^3 \equiv 343 \equiv 3 \pmod{10},
\]
hence \( r = 3 \) is the last digit of the decimal expansion.

**Remark:** For the argument above we do not need the factorization \( 999996 = 4 \cdot 249999 \). It is enough to know that \( 4 \mid 999996 \) which one can check (for example) using the criterion for divisibility by 4. Indeed, write \( 999996 = 4k \); then

\[
7^{999996} = 7^{999996} \cdot 7^3 = (7^4)^k \cdot 7^3 \equiv 343 \equiv 3 \pmod{10},
\]
as above. This is relevant because sometimes it allows to work with very large numbers without having to find factorizations.

**Problem 8.** Let \( a \in \mathbb{Z} \) satisfy \( 3 \nmid a \) or \( 9 \mid a \).

It is a consequence of FLT that \( a^7 \equiv a \pmod{7} \). We claim that \( a^7 \equiv a \pmod{9} \). Note that \( 63 = 7 \cdot 9 \) and \( (7, 9) = 1 \). Then by the CRT we conclude that \( a^7 \equiv a \pmod{63} \), as desired.

We will now prove the claim, dividing into two cases:

- (i) Suppose \( 9 \mid a \); then \( 9 \mid a^7 \) and \( a^7 \equiv 0 \equiv a \pmod{9} \).
- (ii) Suppose \( 3 \nmid a \); then \( (a, 9) = 1 \). We have \( \phi(9) = 6 \) and by Euler’s theorem we have \( a^6 \equiv 1 \pmod{9} \). Thus \( a^7 \equiv a \pmod{9} \), as desired.

**Problem 10.** Let \( a, b \in \mathbb{Z}_{>0} \) be coprime. We have

\[
a^{\phi(b)} \equiv 1 \pmod{b}, \quad a^{\phi(b)} \equiv 0 \pmod{a}
\]

and

\[
b^{\phi(a)} \equiv 1 \pmod{a}, \quad b^{\phi(a)} \equiv 0 \pmod{b}
\]

Thus we also have

\[
a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{a}, \quad a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{b}
\]

and by the CRT we conclude \( a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab} \), as desired.

**Problem 14.** We know from the proof of CRT that the unique solution modulo \( M = m_1 \cdot \ldots \cdot m_n \) to the system of congruences is given by

\[
x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_r M_r y_r \pmod{M}
\]

where \( M_i = M/m_i \) and \( y_i \in \mathbb{Z} \) satisfies \( M_i y_i \equiv 1 \pmod{m_i} \). Now note that \( (M_i, m_i) = 1 \) and Euler’s theorem implies

\[
M_i^{\phi(m_i)} = M_i \cdot M_i^{\phi(m_i)-1} \equiv 1 \pmod{m_i},
\]
hence we can take \( y_i = M_i^{\phi(m_i)-1} \). Inserting in the formula for \( x \) we get

\[
x = a_1 M_1^{\phi(m_1)} + a_2 M_2^{\phi(m_2)} + \ldots + a_r M_r^{\phi(m_r)} \pmod{M},
\]

as desired.
Problem 4. Let $\phi$ be the Euler $\phi$-function. Let $n \in \mathbb{Z}_0$. If $n \neq 1$ it has a prime factorization $n = p_1^{a_1}p_2^{a_2} \cdots p_k^{a_k}$ where $a_k \geq 1$ and $p_i$ are distinct primes. We have

$$\phi(n) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - 1).$$

a) Suppose $\phi(n) = 1$. Since $\phi(1) = 1$ then $n = 1$ is a solution. Suppose $n \neq 1$. From the formula above it follows that $p_i - 1 = 1$ for all $i$; thus 2 is the unique prime factor of $n$, that is $n = 2^{a_1}$. Again by the formula we have $1 = \phi(2^{a_1}) = 2^{a_1-1}$ which implies $a_1 = 1$, hence $n = 2$. Thus $\phi(n) = 1$ if and only if $n = 1$ or $n = 2$.

b) Suppose $\phi(n) = 2$; thus $n 
eq 1$. By the formula $p_i - 1 | 2$ for all $i$; thus only the primes 2 and 3 can divide $n$. Write $n = 2^{a_1}3^{a_2}$; if $a_2 \neq 0$ from the formula we have $3^{a_2-1} | 2$ thus $a_2 = 1$. We conclude that $a_2 = 0$ or $a_2 = 1$. We now divide into two cases:

   (i) Suppose $a_2 = 1$, i.e. $n = 2^{a_1}3$. If $a_1 \geq 2$ then the formula shows that $\phi(n) = 2$ is divisible by 4, a contradiction. We conclude $a_1 \leq 1$, that is $n = 3$ or $n = 6$. Both are solutions because $\phi(3) = \phi(6) = 2$.

   (ii) Suppose $a_2 = 0$, i.e $n = 2^{a_1}$ with $a_1 \geq 1$. Then $\phi(n) = 2^{a_1-1} = 2$ implies $a_1 = 2$, that is $n = 4$.

Thus $\phi(n) = 2$ if and only if $n = 3$, $n = 4$ or $n = 6$.

c) Suppose $\phi(n) = 3$ (hence $n \neq 1$). Then $p_i - 1 = 1$ or 3 for all $i$. Since $p_i = 4$ is not a prime we conclude that $p_i - 1 = 1$; thus only the prime 2 divide $n$, that is $n = 2^{a_1}$ with $a_1 \geq 1$. Therefore $\phi(n) = 2^{a_1-1} = 3$ which is impossible for any value of $a_1$.

Thus there are no solutions to $\phi(n) = 3$.

d) Suppose $\phi(n) = 4$ (hence $n \neq 1$). Again, the formula shows that $p_i - 1 | 4$ for all $i$; thus only the primes 2, 3 and 5 can divide $n$, that is $n = 2^{a_1}3^{a_2}5^{a_3}$ with at least one exponent $\geq 1$. If $a_2 \geq 2$ then $3 | \phi(n) = 4$, a contradiction; thus $a_2 \leq 1$. We now divide into the cases:

   (i) Suppose $a_2 = 1$, i.e. $n = 2^{a_1}3 \cdot 5^{a_3}$. Then

   $$4 = \phi(n) = \phi(3)\phi(2^{a_1}5^{a_3}) = 2\phi(2^{a_1}5^{a_3})$$

   and we conclude $\phi(2^{a_1}5^{a_3}) = 2$. By part (b) the only integers $m$ such that $\phi(m) = 2$ are $m = 3, 4, 6$ and among these only $m = 4$ is of the form $2^{a_1}5^{a_3}$. We conclude that $a_1 = 2$ and $a_3 = 0$ therefore $n = 3 \cdot 4 = 12$.

   (ii) Suppose $a_2 = 0$, i.e. $n = 2^{a_1}5^{a_3}$. Clearly, $a_3 \leq 1$ otherwise $5 | \phi(n) = 4$.

   Suppose $a_3 = 1$, that is $n = 2^{a_1} \cdot 5$. If $a_1 = 0$ then $n = 5$ and $\phi(5) = 4$ is a solution; if $a_1 \geq 1$ then $4 = \phi(n) = 2^{a_1-1} \cdot 4$ implies $a_1 = 1$, that is $n = 10$.

   Suppose $a_3 = 0$, that is $n = 2^{a_1}$ with $a_1 \geq 1$. Thus $\phi(n) = 2^{a_1-1} = 4$ implies $a_1 = 3$ that is $n = 8$.

Thus $\phi(n) = 4$ if and only if $n = 5, 8, 10$ or 12.
Problem 8. Suppose $\phi(n) = 14$; hence $n > 1$. Consider the prime factorization $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ where $a_k \geq 1$ and $p_i$ are distinct primes. We have

$$\phi(n) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - 1).$$

From the formula it follows $p_i - 1 \mid 14$ for each prime $p_i \mid n$, that is $p_i - 1 \in \{1, 2, 7, 14\}$; thus $p_i = 2, 3, 8, 15$ and we conclude that only the primes 2 and 3 can divide $n$. Write $n = 2^{a_1} 3^{a_2}$. We have $\phi(n) = \phi(2^{a_1})\phi(3^{a_2}) = 14$, but from the formula we see that $7 \nmid \phi(2^{a_1})$ and $7 \nmid \phi(3^{a_2})$, a contradiction.

Thus $\phi(n) = 14$ has no solutions.

Problem 18. Let $n \in \mathbb{Z}_{>0}$ be odd; then $(4, n) = 1$. Since $\phi$ is a multiplicative function we have $\phi(4n) = \phi(4)\phi(n) = 2\phi(n)$, as desired.