**Homework Set 9**

**Math 221 — Winter 2016**

*Do not turn in.*

**Problem 9.1. a)** Compute $10\%7$, $100\%7$, $1000\%7$, $10000\%7$, $100000\%7$, $1000000\%7$.

b) Use part a) to quickly determine $9001073\%7$.

**Answer.**

a) $10\%7 = 3$, $100\%7 = 2$, $1000\%7 = 6$, $10000\%7 = 4$, $100000\%7 = 5$, $1000000\%7 = 1$.

b) $9001073 = 9(1000000) + 1(1000) + 7(10) + 3 \equiv 9 \cdot 1 + 1 \cdot 6 + 7 \cdot 3 + 3 \equiv 2 \cdot 1 + 1 \cdot 6 + 0 \cdot 3 + 3 \equiv 11 \equiv 4 \mod 7$.

**Problem 9.2.** Use the extended Euclidean algorithm to compute $\gcd(342, 232)$; show each intermediate step in the algorithm and use this to find integers $x$ and $y$ such that $342x + 232y = \gcd(342, 232)$. Do the same for $\gcd(1714, 1814)$.

**Answer.**

\[
\gcd(342, 232) = \gcd(342 - 232, 232)
\]
\[
= \gcd(342 - 232, 2(342 - 232))
\]
\[
= \gcd(342 - 232, 3(232 - 2 \cdot 342))
\]
\[
= \gcd((19)342 - (28)232, 3 \cdot 232 - 2 \cdot 342)
\]
\[
= 2.
\]

$342(19) + 232(-28) = 2 = \gcd(342, 232)$. 


gcd(1714, 1814) = gcd(1714, 1814 − 1714)

= gcd(1714 − 17(1814 − 1714), 1814 − 1714)

= gcd((18)1714 − (17)1814, 1814 − 1714)

= gcd((18)1714 − (17)1814, 1814 − 1714 − 7((18)1714 − (17)1814))

= gcd((18)1714 − (17)1814, (120)1814 − (127)1714)

= 2

1814(120) + 1714(−127) = 2 = gcd(1814, 1714).

Problem 9.3. An element \( k \) of \( \mathbb{Z}_n \) is invertible if there is an \( a \in \mathbb{Z}_n \) such that \( ka \equiv 1 \mod n \). Find the inverses of all the invertible elements of \( \mathbb{Z}_{26} \).

Answer. The invertible elements of \( \mathbb{Z}_{26} \) are the elements \( k \) such that \( \gcd(k, 26) = 1 \), which are the elements whose prime factorizations do not involve 2 or 13. These are 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.

<table>
<thead>
<tr>
<th>( k )</th>
<th>( k^{-1} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>7</td>
<td>15</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>11</td>
<td>19</td>
</tr>
<tr>
<td>15</td>
<td>7</td>
</tr>
<tr>
<td>17</td>
<td>23</td>
</tr>
<tr>
<td>19</td>
<td>11</td>
</tr>
<tr>
<td>21</td>
<td>5</td>
</tr>
<tr>
<td>23</td>
<td>17</td>
</tr>
<tr>
<td>25</td>
<td>25</td>
</tr>
</tbody>
</table>

Problem 9.4. Do there exist integers \( x \) and \( y \) such that \( 4x + 6y = 2 \)? Either find a solution or say why none exists.

Answer. Yes, the extended Euclidean algorithm will find them:

\[
gcd(4, 6) = gcd(4, 6 - 4) = 2.
\]

Thus

\[
4(-1) + 6(1) = 2.
\]
**Problem 9.5.** Do there exist integers \( x \) and \( y \) such that \( 4x + 6y = 3 \)? Either find a solution or say why none exists.

*Answer.* No. If \( 4x + 6y = 3 \), then \( \gcd(4, 6) \mid 3 \), but this is untrue.

**Problem 9.6.** Compute \( \phi(n) \) for \( n = 2, 3, 4, 5, 6, 27, 30, 100, 400, 100000 \).

*Answer.*

\[
\begin{align*}
\phi(2) &= 2 - 1 = 1 \\
\phi(3) &= 3 - 1 = 2 \\
\phi(4) &= \phi(2^2) = 2^2 - 2 = 2 \\
\phi(5) &= 5 - 1 = 4 \\
\phi(6) &= \phi(2)\phi(3) = (2 - 1)(3 - 1) = (1)(2) = 2 \\
\phi(27) &= \phi(3^3) = 3^3 - 3^2 = 18 \\
\phi(30) &= \phi(2)\phi(3)\phi(5) = (2 - 1)(3 - 1)(5 - 1) = (1)(2)(4) = 8 \\
\phi(100) &= \phi(2^2)\phi(5^2) = (2^2 - 2)(5^2 - 5) = (2)(20) = 40 \\
\phi(400) &= \phi(2^4)\phi(5^2) = (2^4 - 2^3)(5^2 - 5) = (8)(20) = 160 \\
\phi(100000) &= \phi(2^55^5) = (2^5 - 2^4)(5^5 - 5^4) = (16)(2500) = 40000
\end{align*}
\]

**Problem 9.7.** Prove or disprove: \( \phi(ab) = \phi(a)\phi(b) \) for all integers \( a, b > 1 \).

*Answer.* False. \( \phi(6 \cdot 2) = \phi(12) = |\{1, 5, 7, 11\}| = 4 \), but \( \phi(6) = |\{1, 5\}| = 2 \) and \( \phi(2) = |\{1\}| = 1 \), and \( 4 \neq 2 \cdot 1 \).

**Problem 9.8.** Let \( p \) be a prime. Note that \( D(p^2) = \{\pm 1, \pm p, \pm p^2\} \).

a) Determine the set of integers \( \{k \in \mathbb{Z} : \gcd(k, p^2) = p \text{ and } 1 \leq k < p^2\} \).

b) Determine the set of integers \( \{k \in \mathbb{Z} : \gcd(k, p^2) = 1 \text{ and } 1 \leq k < p^2\} \).

c) Use part (b) to show that \( \phi(p^2) = p^2 - p \).

*Answer.*

a) If \( k \) is a multiple of \( p \), then \( p|k \) and \( p|p^2 \). Since the only divisors of \( p^2 \) are \( \pm 1, \pm p, \pm p^2 \), and \( k < p^2 \) (thus \( p^2 \nmid k \)), so \( p = \gcd(k, p^2) \). On the other hand, if \( k \) is not a multiple of \( p \), then \( \gcd(k, p^2) = 1 \). Thus this set is \( \{p, 2p, 3p, \ldots, (p - 1)p\} \).

b) Since the only divisors of \( p^2 \) are \( \pm 1, \pm p, \pm p^2 \), this set is

\[
B := \{1, 2, \ldots, p^2 - 1\} - A,
\]

where \( A \) denotes the set in part (a). Explicitly, this set is

\[
\{1, 2, 3, \ldots, p-1, p+1, p+2, \ldots, 2p-1, 2p+1, \ldots, (p-1)p-1, (p-1)p+1, (p-1)p+2, \ldots, p^2-1\}.
\]
c) \( \phi(p^2) = |B| = |\{1, 2, \ldots, p^2 - 1\}| - |A| = (p^2 - 1) - (p - 1) = p^2 - p \), where the second equality is because \( A \subseteq \{1, 2, \ldots, p^2 - 1\} \).

**Problem 9.9.** Without using a calculator, compute \( 10^{6004} \mod 7 \). Hint: Use Fermat’s little theorem.

**Answer.** By Fermat’s Little Theorem, \( 10^{7-1} = 10^6 \equiv 1 \mod 7 \). Since \( 6004 = 6(1000) + 4 \), we compute

\[
10^{6004} = 10^{6 \cdot 1000 + 4} \\
= (10^6)^{1000}10^4 \\
\equiv (1)^{1000}10^4 \\
\equiv 10^4 \\
\equiv 3^4 \\
\equiv 81 \\
\equiv 4 \mod 7
\]

**Problem 9.10.** Euler’s generalization of Fermat’s little theorem says that \( a^{\phi(n)} \equiv 1 \mod n \) if \( \gcd(a, n) = 1 \). Use this to find the last 5 digits of \( 7^{40000} \).

**Answer.** The last 5 digits of \( 7^{40000} \) is computed by \( 7^{40000} \mod 100000 \). We have \( \gcd(100000, 7) = \gcd(2^5 \cdot 5^5, 7) = 1 \) and \( \phi(100000) = 40000 \). Thus, applying Euler’s generalization of Fermat’s little theorem,

\[
7^{40000} = 7^{\phi(100000)} \equiv 1 \mod 100000,
\]

thus the last five digits are 00001.