Midterm (Take Home)

You must upload the solutions to this exam by 11:59pm on Tuesday 06/16. Since this is a take home, I want all your solutions to be neat and well written.

You can look at your notes, class discussions on SMC, *our* book, our videos and solutions posted by me, but you cannot look at any other references (including the Internet) and you cannot discuss this with *anyone*!

You can use a computer only to check your answers, as **you need to show work in all questions**.

1) [15 points] Use the *Extended Euclidean Algorithm* to write the GCD of 1183 and 826 as a linear combination of themselves. *Show the computations explicitly!* [**Hint:** You should get 7 for the GCD!]

Solution. We have:

$$\begin{aligned}
1138 &= 826 \cdot 1 + 357 \\
826 &= 357 \cdot 2 + 112 \\
357 &= 112 \cdot 3 + 21 \\
112 &= 21 \cdot 5 + 7 \\
21 &= 7 \cdot 3.
\end{aligned}$$

So $\gcd(1138, 357) = 7$. Now,

$$\begin{aligned}
7 &= 112 - 5 \cdot 21 \\
&= 112 - 5 \cdot (357 - 3 \cdot 112) = -5 \cdot 357 + 16 \cdot 112 \\
&= -5 \cdot 357 + 16 \cdot (826 - 2 \cdot 357) = 16 \cdot 826 - 37 \cdot 357 \\
&= 16 \cdot 826 - 37 \cdot (1138 - 826) = \boxed{-37} \cdot 1138 + \boxed{53} \cdot 826
\end{aligned}$$

□

2) [13 points] Compute the LCM of 1183 and 826 [the same numbers above!].

Solution. We have:

$$\begin{aligned}
\operatorname{lcm}(1183, 826) &= \frac{1183 \cdot 826}{\gcd(1183, 826)} \\
&= \frac{1183 \cdot 826}{7} \\
&= 169 \cdot 826 = \boxed{139594}.
\end{aligned}$$

□

3) [15 points] Find the remainder of the division of 9482^{1532} when divided by 5 [i.e., what is 9482^{1532} congruent to modulo 5]. *Show your computations explicitly!*

Solution. We have:

$$\begin{aligned}1532 &= 5 \cdot 306 + 2\\ 306 &= 5 \cdot 61 + 1\\ 61 &= 5 \cdot 12 + 1\\ 12 &= 5 \cdot 2 + 2\\ 2 &= 5 \cdot 0 + 2.\end{aligned}$$

So, $1532 = 2 + 1 \cdot 5 + 1 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4$. Also, note that $2 + 1 + 1 + 2 + 2 = 8 = 3 + 1 \cdot 5$.

Thus, using Fermat's Theorem, we have:

$$9482^{1532} \equiv 2^{15432} \equiv 2^{2+1+1+2+2} = 2^8 \equiv 2^{3+1} = 2^4 = 16 \equiv 1 \pmod 5.$$

□

4) [15 points] Give the set of all solutions of the system

$$\begin{aligned}4x &\equiv 5 \pmod{15}\\ 5x &\equiv 22 \pmod{33}\end{aligned}$$

[**Hint:** The system *does* have solution(s)!]

Solution. We first clear the coefficients of x: we have that $4 \cdot 4 \equiv 1 \pmod{15}$, so the first equation becomes:

$$x \equiv 20 \equiv 5 \pmod 5.$$

Also, we have that $-13 \cdot 5 = -65 \equiv 1 \pmod{33}$. [We can find this using the Extended Euclidean Algorithm.] So, the second equation becomes:

$$x \equiv -286 \equiv 11 \pmod{33}.$$

So, we have the system:

$$\begin{aligned}x &\equiv 5 \pmod{15}\\ x &\equiv 11 \pmod{33}.\end{aligned}$$

Since $\gcd(15, 33) = 3$ and $3 \mid (5 - 11)$, we know that the system has solution.

From the first equation, we have that $x = 5 + 15 \cdot k$, for $k \in \mathbb{Z}$. Substituting in the second we get $5 + 15k \equiv 11 \pmod{33}$, or $15k \equiv 6 \pmod{33}$. Now, we have $\gcd(15, 33) = 3$ and $3 \mid 6$, so we divide through by 3, and get $5k \equiv 2 \pmod{11}$. Since $-2 \cdot 5 = -10 \equiv 1 \pmod{11}$, we get $k \equiv -4 \equiv 7 \pmod{11}$. Thus, $k = 7 + 11l$, for $l \in \mathbb{Z}$.

Replacing this back in the formula for x, we get $x = 5 + 15 \cdot (7 + 11 \cdot l) = 110 + 165 \cdot l$, for $l \in \mathbb{Z}$, which is our solution set. □

5) [12 points] Suppose that

$$\begin{aligned} m &= 2^a \cdot 3^2 \cdot 5^b \cdot 7^3, \\ n &= 2^5 \cdot 3^c \cdot 5^4 \cdot 7^d, \\ \gcd(m, n) &= 2^5 \cdot 3^2 \cdot 5 \cdot 7^2, \\ \operatorname{lcm}(n, m) &= 2^7 \cdot 3^2 \cdot 5^4 \cdot 7^3. \end{aligned}$$

Find a, b, c and d.

Solution. By the formulas for GCD and LCM using the Fundamental Theorem of Arithmetic, we have [for the prime 2] that $5 = \min(a, 5)$ and $7 = \max(a, 5)$, so $a = 7$.

Similarly, for the prime 3, we have that $2 = \min(2, c)$ and $2 = \max(2, c)$, and hence $c = 2$.

For the prime 5, we have that $1 = \min(b, 4)$ and $4 = \max(b, 4)$, and hence $c = 1$.

Finally, for the prime 7, we have that $2 = \min(3, d)$ and $3 = \max(3, d)$, and hence $d = 2$. □

6) [15 points] Let a, b and c be positive integers and suppose that there are $r, s, t \in \mathbb{Z}$ such that

$$ra + sb + tc = 1.$$

Prove that $\gcd(a, b, c) = 1$.

Solution. Let $d \stackrel{\text{def}}{=} \gcd(a, b, c)$. Since $d \mid a$, we also have that $d \mid ra$. Similarly, since $d \mid b, c$, we also have that $d \mid (sb), (tc)$. Thus, $d \mid (ra + sb + tc) = 1$. Since $d > 0$ and a divisor of 1, we must have that $d = 1$. □

7) [15 points] Let p be a prime. Prove that for any integer a such that $p \nmid a$, the equation $x^p - x + a = 0$ never has an *integral* [i.e., in $\mathbb{Z}$] solution.

[**Hint:** As I've mentioned before, if an equation has an integral solution, it has a solution modulo any m.]

Proof. By Fermat's Theorem, for any $b \in \mathbb{Z}$, we have, since p is prime, that

$$b^p \equiv b \pmod{p}$$

So, if b is an integral solution of the equation, we have

$$0 = b^p - b + a \equiv b - b + a = a \pmod{p},$$

i.e., $a \equiv 0 \pmod{p}$. Thus, this would mean that $p \mid a$, which is not the case. So the equation cannot have an integral solution. [If it did, then we would have $p \mid a$.] □