Second exam for Math 463

Prof. Bernardo Ábrego May 1st, 2014.

Time limit: 75 minutes. Problems 1–5 are worth 20 points each, Problem 6 is worth 10 extra points. All your answers must be justified. Good luck!
In the following problems all variables are integers

1. Solve the following equations:

   (a) $353x \equiv 254 \pmod{400}$.
   Because $400 = 16 \cdot 25$, the equation is equivalent to solving the system

   $$353x \equiv 254 \pmod{16} \qquad \text{and} \qquad 353x \equiv 254 \pmod{25},$$

   which after reducing is equivalent to

   $$x \equiv 14 \pmod{16} \qquad \text{and} \qquad 3x \equiv 4 \pmod{25}.$$

   Multiplying the second equation by 8 yields $-x \equiv 24x \equiv 32 \equiv -18 \pmod{25}$. Thus $x = 18 + 25t$ for some integer t. Plugging in the 1st equation yields $25t \equiv -4 \pmod{16}$, which is equivalent to $9t \equiv -4 \pmod{16}$. Multiplying by -7 gives $t \equiv -63t \equiv 28 \equiv 12 \pmod{16}$. Thus $x = 18 + 25 \cdot (16k + 12) = 318 + 400k$ for some integer k. Thus the solution is $x \equiv 318 \pmod{400}$.

   (b) $x^3 + x + 57 \equiv 0 \pmod{5^3}$
   Let $f(x) = x^3 + x + 57$. First we solve the equation modulo 5. Note that $f(0) = 57 \equiv 2 \pmod 5$, $f(1) = 59 \equiv 4 \pmod 5$, $f(2) = 67 \equiv 2 \pmod 5$, $f(-2) = 47 \equiv 2 \pmod 5$, and $f(-1) = 55 \equiv 0 \pmod 5$. Thus the only solution modulo 5 is $x \equiv 4 \pmod 5$. Let $a = 4$. Note that $f'(a) = f'(4) = 3 \cdot 4^2 + 1 \equiv 4 \pmod 5$. Thus by Hensel's Lemma this solution will lift to a unique solution modulo 25, and then to a unique solution modulo 125. Note that $\overline{f'(4)} = 4$, and thus

   $$\begin{aligned} a_1 &= a - f(a)\overline{f'(4)} = 4 - 125 \cdot 4 \equiv 4 \pmod{25}, \text{ and} \\ a_2 &= a_1 - f(a_1)\overline{f'(4)} = 4 - 125 \cdot 4 \equiv 4 \pmod{125}. \end{aligned}$$

   So the solution is $x \equiv 4 \pmod{5^3}$

2. Let m and n be two positive integers and let P be the product of the primes that divide both m and n. Prove that
$$\phi(mn)\phi(P) = P\phi(m)\phi(n).$$

   Note that $\phi(m) = m\prod_{p|m}(1 - 1/p)$ and $\phi(n) = n\prod_{p|n}(1 - 1/p)$. Also, the product $\prod_{p|m}(1 - 1/p) \cdot \prod_{p|n}(1 - 1/p)$ has a double factor for every prime that divides both m and n, and a single factor otherwise. Thus

$$\begin{aligned} \prod_{p|m}(1 - 1/p) \cdot \prod_{p|n}(1 - 1/p) &= \left[\prod_{p|P}(1 - 1/p)\right]^2 \cdot \prod_{\substack{p|n \\ p\nmid P}}(1 - 1/p) \cdot \prod_{\substack{p|m \\ p\nmid P}}(1 - 1/p) \\ &= \left[\prod_{p|P}(1 - 1/p)\right]^2 \cdot \prod_{\substack{p|mn \\ p\nmid P}}(1 - 1/p)\,. \end{aligned}$$

Therefore

$$\begin{aligned}
P\phi(m)\phi(n) &= Pmn \prod_{p|m}(1-1/p)\cdot\prod_{p|n}(1-1/p)\\
&= Pmn\left[\prod_{p|P}(1-1/p)\right]^2 \cdot \prod_{\substack{p|mn\\ p\nmid P}}(1-1/p)\\
&= P\left[\prod_{p|P}(1-1/p)\right]\cdot mn\prod_{p|mn}(1-1/p)\\
&= \phi(P)\phi(mn).
\end{aligned}$$

3. Find all primes q for which 5 is not a quadratic residue.

   If $q=2$, then $1^2 \equiv 5 \pmod 2$, so 5 is a quadratic residue modulo 2. Obviously 5 is also a quadratic residue modulo 5. If q is odd and relatively prime to 5, then by the quadratic reciprocity law,

   $$\left(\frac{5}{q}\right) = \left(\frac{q}{5}\right)(-1)^{(5-1)/2\cdot(q-1)/2} = \left(\frac{q}{5}\right)(-1)^{2\cdot(q-1)/2} = \left(\frac{q}{5}\right).$$

   Thus $\left(\frac{5}{q}\right) = -1$ if and only if $\left(\frac{q}{5}\right)$. Because the only nonresidues modulo 5 are 2 and 3, it follows that $\left(\frac{5}{q}\right) = -1$ if and only if q is a prime congruent to 2 or 3 modulo 5.

4. Suppose that $b \equiv a^{31} \pmod{91}$ and that $\gcd(a, 91) = 1$. Find a positive number k such that $b^k \equiv a \pmod{91}$.

   Note that $91 = 13\cdot 7$ and so $\phi(91) = \phi(13)\cdot\phi(7) = 12\cdot 6 = 72 = 2^3\cdot 3^2$. We solve the equation $31x \equiv 1 \pmod{72}$. Because $72 = 2\cdot 31+10$, and $31 = 3\cdot 10+1$, it follows that $1 = 31-3\cdot(72-2\cdot 31) = 7\cdot 31-3\cdot 72$. Thus $k = x \equiv 7 \pmod{72}$ is the desired solution. To verify that it works note that

   $$b^7 \equiv \left(a^{31}\right)^7 = a^{3\cdot 72+1} = \left(a^{72}\right)^3\cdot a \equiv 1^3\cdot a \pmod{91},$$

   because $a^{\phi(91)} = a^{72} \equiv 1 \pmod{91}$ for relatively prime a to 91.

5. (Extra) Show that $(x^2-2)/(2y^2+3)$ is never an integer when x and y are integers.

   Suppose that $(x^2-2)/(2y^2+3) = n$ is an integer. It follows that $x^2 \equiv 2 \pmod{n(2y^2+3)}$ and so $x^2 \equiv 2 \pmod{2y^2+3}$. Therefore the Jacobi symbol $\left(\frac{2}{2y^2+3}\right) = 1$. (Note that $2y^2+3$ is positive and odd)

   However,

   $$\left(\frac{2}{2y^2+3}\right) = (-1)^{((2y^2+3)^2-1)/8},$$

   and

   $$\frac{(2y^2+3)^2-1}{8} = \frac{(2y^2+4)(2y^2+2)}{8} = \frac{(y^2+2)(y^2+1)}{2}.$$

   Finally note that if y is even, then $(y^2+2)(y^2+1) \equiv 2 \pmod 4$, and if y is odd, then $y^2 \equiv 1 \pmod 4$ and $(y^2+2)(y^2+1) \equiv 3\cdot 2 \equiv 2 \pmod 4$. In any case the conclusion is that $((2y^2+3)^2-1)/8$ is odd and so

   $$\left(\frac{2}{2y^2+3}\right) = -1,$$

   which is a contradiction.