Math 406 Exam 3 Summer 2016 Solutions

---

1. Evaluate each of the following:

   (a) $\left(\frac{19}{45}\right)$

   Solution: Observe:

   $\left(\frac{19}{45}\right) = \left(\frac{45}{19}\right) = \left(\frac{7}{19}\right) = -\left(\frac{19}{7}\right) = -\left(\frac{5}{7}\right) = -\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right) = -(-1)^{(5^2-1)/8} = 1$

   (b) $\left(\frac{1001}{9907}\right)$

   Solution: Observe:

   Step 1: $\left(\frac{1001}{9907}\right) = \left(\frac{9907}{1001}\right) = \left(\frac{898}{1001}\right) = \left(\frac{2}{1001}\right)\left(\frac{449}{1001}\right)$.

   Step 2: $\left(\frac{2}{1001}\right) = \left(\frac{2}{7}\right)\left(\frac{2}{11}\right)\left(\frac{2}{13}\right) = (-1)^{(7^2-1)/8}(-1)^{(11^2-1)/8}(-1)^{(13^2-1)/8} = (1)(-1)(-1) = 1$.

   Step 3: $\left(\frac{449}{1001}\right) = \left(\frac{1001}{449}\right) = \left(\frac{103}{449}\right) = \left(\frac{449}{103}\right) = \left(\frac{37}{103}\right) = \left(\frac{103}{37}\right) = \left(\frac{29}{37}\right) = \left(\frac{37}{29}\right) = \left(\frac{8}{29}\right) = \left(\frac{2}{29}\right)^3 = \left((-1)^{(29^2-1)/8}\right)^3 = -1$.

   Finally: $\left(\frac{1001}{9907}\right) = (1)(-1) = -1$

2. A partial table of indices for 2, a primitive root of 13 is given here:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_2 a$	12	1	4	2	9	5	11	3	a	b	7	6

   (a) Find a and b with justification.

   Solution: We have $a \equiv \text{ind}_2 9 \equiv \text{ind}_2(3^2) \equiv 2\text{ind}_2 3 \equiv 8 \bmod 12$ and $b \equiv \text{ind}_2 10 \equiv \text{ind}_2(2 \cdot 5) \equiv \text{ind}_2 2 + \text{ind}_2 5 \equiv 1 + 9 \equiv 10 \bmod 12$.

   (b) Use the table to solve the congruence $3^{2x+1} \equiv 9 \bmod 13$.

   Solution: We have:

$$\begin{aligned}
3^{2x+1} &\equiv 9 \bmod 13 \\
\text{ind}_2\left(3^{2x+1}\right) &\equiv \text{ind}_2 9 \bmod 12 \\
(2x+1)\text{ind}_2 3 &\equiv \text{ind}_2 9 \bmod 12 \\
(2x+1)(4) &\equiv 8 \bmod 12 \\
8x &\equiv 4 \bmod 12 \\
2x &\equiv 1 \bmod 3 \\
x &\equiv 2 \bmod 3
\end{aligned}$$

   (c) Use the table to solve the congruence $7x^5 \equiv 3 \bmod 13$.

   Solution: We have

$$\begin{aligned}
7x^5 &\equiv 3 \bmod 13 \\
\text{ind}_2(7x^5) &\equiv \text{ind}_2 3 \bmod 12 \\
\text{ind}_2 7 + 5\text{ind}_2 x &\equiv \text{ind}_2 3 \bmod 12 \\
11 + 5\text{ind}_2 x &\equiv 4 \bmod 12 \\
5\text{ind}_2 x &\equiv 5 \bmod 12 \\
\text{ind}_2 x &\equiv 1 \bmod 12 \\
x &\equiv 2 \bmod 13
\end{aligned}$$

3. For each $1 \leq a \leq 15$ with $\gcd(a, 15) = 1$ find and justify $\text{ord}_{15}a$.

   Solution: The orders must divide $\phi(15) = 8$ so the options are 1,2,4,8.

   $1^1 \equiv 1 \bmod 15$ so $\text{ord}_{15}1 = 1$.
   $2^1 \equiv 2 \bmod 15$, $2^2 \equiv 4 \bmod 15$, $2^4 \equiv 1 \bmod 15$ so $\text{ord}_{15}2 = 4$.
   $4^1 \equiv 4 \bmod 15$, $4^2 \equiv 1 \bmod 15$ so $\text{ord}_{15}4 = 2$.
   $7^1 \equiv 7 \bmod 15$, $7^2 \equiv 4 \bmod 15$, $7^4 \equiv 1 \bmod 15$ so $\text{ord}_{15}4 = 4$.
   $8^1 \equiv 8 \bmod 15$, $8^2 \equiv 4 \bmod 15$, $8^4 \equiv 1 \bmod 15$ so $\text{ord}_{15}8 = 4$.
   $11^1 \equiv 11 \bmod 15$, $11^2 \equiv 1 \bmod 15$ so $\text{ord}_{15}11 = 2$.
   $13^1 \equiv 13 \bmod 15$, $13^2 \equiv 4 \bmod 15$, $13^4 \equiv 1 \bmod 15$ so $\text{ord}_{15}13 = 4$.
   $14^1 \equiv 14 \bmod 15$, $14^2 \equiv 1 \bmod 15$ so $\text{ord}_{15}14 = 2$.

4. Suppose that Bob's public key is $(e, n) = (3, 33)$.

   (a) Encrypt the message `CAFE` using 1-character blocks.

   Solution: We have:

   `C` has $P = 2$ so $C \equiv 2^3 \equiv 08 \bmod 33$.
   `A` has $P = 0$ so $C \equiv 0^3 \equiv 00 \bmod 33$.
   `F` has $P = 5$ so $C \equiv 5^3 \equiv 26 \bmod 33$.
   `E` has $P = 4$ so $C \equiv 4^3 \equiv 31 \bmod 33$.

   So the ciphertext is `08 00 26 31`.

   (b) Since you are so smart you can factor n and find $\phi(n)$. Do so, then calculate Bob's private key d.

   Solution: We have $\phi(33) = \phi(3)\phi(11) = (2)(10) = 20$ we then need to solve $3d \equiv 1 \bmod 20$. The answer is obviously $d \equiv 7 \bmod 20$.

   (c) Decrypt the single ciphertext `04`.

   Solution: We have $04^7 \equiv 16 \bmod 33$ so the message was `Q`.

5. The ciphertext `MOOHCHHXBOO` was created using an affine cipher. Perform frequency analysis and decrypt.

   Solution: The most common letter is `O` which probably represents `E` and the second most common letter is `H` which probably represents `T`. Thus we solve:

$$\begin{aligned}
4a + b &\equiv 14 \bmod 26 \\
19a + b &\equiv 7 \bmod 26 \\
15a &\equiv -7 \bmod 26 \\
(3)(5)a &\equiv -7 \bmod 26 \\
(9)(3)(5)a &\equiv (9)(-7) \bmod 26 \\
5a &\equiv 15 \bmod 26 \\
a &\equiv 3 \bmod 26
\end{aligned}$$

   So then $4(3) + b \equiv 14 \bmod 26$ so that $b \equiv 2 \bmod 26$. We find $a^{-1} \equiv 9 \bmod 26$ and decrypt the letters we don't know:

   `M` has $C = 12$ so $P \equiv 9(12 - 2) \equiv 12 \bmod 26$ so `M`.
   `C` has $C = 2$ so $P \equiv 9(2 - 2) \equiv 0 \bmod 26$ so `A`.
   `X` has $C = 23$ so $P \equiv 9(23 - 2) \equiv 7 \bmod 26$ so `H`.
   `B` has $C = 1$ so $P \equiv 9(1 - 2) \equiv 17 \bmod 26$ so `R`.

   So the message is `MEETATTHREE`.

6. Determine whether 15 is a quadratic residue of 17:

   (a) Using Euler's Criterion.

   Solution:

   $$\left(\frac{15}{17}\right) \equiv (15)^{(17-1)/2} \equiv (-2)^8 \equiv 256 \equiv 1 \bmod 17$$

   so yes.

   (b) Using Gauss' Lemma.

   Solution: $\{1(15), 2(15), ..., 8(15)\} \equiv \{15, 13, 11, 9, 7, 5, 3, 1\} \bmod 17$ of which $s = 4$ are greater than $\frac{17}{2} = 8.5$. Thus $\left(\frac{15}{17}\right) = (-1)^4 = 1$ so yes.

7. Prove that if $\mathrm{ord}_n a = hk$ then $\mathrm{ord}_n \left(a^h\right) = k$.

   Solution:

   By a theorem from class:

   $$\mathrm{ord}_n(a^h) = \frac{\mathrm{ord}_n a}{\gcd(\mathrm{ord}_n a, h)} = \frac{hk}{\gcd(hk, h)} = \frac{hk}{h} = k$$

8. Let r be a primitive root for an odd prime p. Prove that $\mathrm{ind}_r(p-1) = \frac{1}{2}(p-1)$.

   Solution: This was HW9.4 #8 so the solution is there.

9. Suppose p and q are distinct odd primes. Prove that there is always some n with $\left(\frac{n}{pq}\right) = -1$.

   Solution:

   We know that $\left(\frac{n}{pq}\right) = \left(\frac{n}{p}\right)\left(\frac{n}{q}\right)$. Let n_1 be a QR of p which exists because there are $\frac{p-1}{2}$ QR of p and $\frac{p-1}{2}$ QNR of p and let n_2 be a QNR of q which exists for similar reasons. Then choose n satisfying

   $$n \equiv n_1 \bmod p$$
   $$n \equiv n_2 \bmod q$$

   which can be done by the CRT. Then

   $$\left(\frac{n}{pq}\right) = \left(\frac{n}{p}\right)\left(\frac{n}{q}\right) = \left(\frac{n_1}{p}\right)\left(\frac{n_2}{q}\right) = (1)(-1) = -1$$

10. Suppose p is an odd prime such that there is some a so that a is a quadratic residue of p but $2a$ is a quadratic non-residue of p. Prove that $p \equiv \pm 3 \bmod 8$.

    Solution: If a is a QR of p but $2a$ is a QNR of p then $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{2a}{p}\right) = -1$. However $\left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a}{p}\right)$ so then $\left(\frac{2}{p}\right) = -1$.

    We could only have $p \equiv \pm 3 \bmod 8$ or $p \equiv \pm 1 \bmod 8$.

    • If $p \equiv \pm 3 \bmod 8$ then $p = 8k \pm 3$ so then $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = (-1)^{(64k^2 \pm 48k + 9 - 1)/8} = -1$ as desired.

    • If $p \equiv \pm 1 \bmod 8$ then $p = 8k \pm 1$ so then $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = (-1)^{(64k^2 \pm 16k + 1 - 1)/8} = 1$.