MA1301 Final Exam Solution Guide

Problem 1: First, Find GCD(286,106) using Euclidean algorithm, and extract a particular solution to the equation $286x+106y=2$.

$$286 = 3\cdot 106 - 32$$
$$106 = 3\cdot 32 + 10$$
$$32 = 3\cdot 10 + 2$$
$$10 = 2\cdot 5 + 0$$

This is a variation on the textbook algorithm, which often terminates faster.

Now finding particular soln to $286x+106y=2$ by "working backwards":

$$\begin{aligned}
2 &= 32 - 3\cdot 10 \\
&= 32 - 3\cdot(106 - 3\cdot 32) \\
&= 32 - 3\cdot 106 + 9\cdot 32 \\
&= 10\cdot 32 - 3\cdot 106 \\
&= 10\cdot(3\cdot 106 - 286) - 3\cdot 106 \\
&= 30\cdot 106 - 10\cdot 286 - 3\cdot 106 \\
&= 286\cdot(-10) + 106\cdot(27)
\end{aligned}$$

This implies

$$14 = 286\cdot(-70) + 106\cdot(189)$$

So $x=-70$ and $y=189$ is a particular solution to the equation $286x+106y=14$. The general solution is then given by

$$x = -70 + 53t$$
$$y = 189 - 145t$$

for all $t \in \mathbb{Z}$.

Problem 2:

1. The Euler phi function is defined for a natural number n to be:

$\phi(n)$ is the number of natural numbers $1 \leq k \leq n$ for which $GCD(n,k) = 1$.

2. Euler's Generalization of Fermat's Little Theorem states that for $n \in \mathbb{N}$ and a an integer that satisfies $GCD(a,n) = 1$ that

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

3. The Euler ϕ-function is multiplicative. Observe $325 = 5^2 \cdot 13$. Thus

$$\phi(325) = \phi(5^2 \cdot 13) = \phi(5^2) \cdot \phi(13) = (5^2 - 5) \cdot (13 - 1) = 20 \cdot 12 = 240.$$

4. We can solve the problem by reducing 3^{482} to a standard residue modulo 325. As $482 = 2 \cdot 240 + 2$, we can use Euler's theorem to see

$$3^{482} \equiv 3^{2 \cdot 240 + 2} \equiv \left(3^{240}\right)^2 \cdot 3^2 \equiv 1^2 \cdot 3^2 \equiv 9 \pmod{325}.$$

Hence the remainder of dividing 3^{482} by 325 is 9.

$=$

Problem 3:

1. Let p be an odd prime and let $a \in \mathbb{Z}$ be relatively prime to p.

Then $$(a|p) = \begin{cases} +1 & \text{if } x^2 \equiv a \pmod p \text{ admits a solution} \\ -1 & \text{if } \text{" } \text{" } \text{ does not have a solution.} \end{cases}$$

2. The Law of Quadratic Reciprocity states that if p and q are two distinct odd primes that $$(p|q)\cdot(q|p) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Equivalently, $$(p|q) = \begin{cases} (q|p) & \text{if } p \equiv 1 \bmod 4 \text{ or } q \equiv 1 \bmod 4 \\ -(q|p) & \text{if } p \equiv 3 \bmod 4 \text{ and } q \equiv 3 \bmod 4. \end{cases}$$

3. Many possible methods:

$(31|13) = (5|13)$ (reduce mod 13)

$= (13|5)$ (quadratic reciprocity, $5 \equiv 1 \bmod 4$)

$= (3|5)$ (reduce mod 5)

$= -1$ by direct verification: $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 4$, $4^2 \equiv 1 \bmod 5$.

$\equiv 3^{\frac{5-1}{2}} \bmod 5$ (Euler's criterion).

$\equiv 3^2 \bmod 5 \equiv -1 \bmod 5.$

$(13|31) = (31|13)$ by Q.R. as $13 \equiv 1 \bmod 4$.

4. ~~$(621|17) = (2|17)\cdot(31|17)$ (multiplicativity)~~

~~$= 1 \cdot (31|17)$ (as $17 \equiv 1 \bmod 8 \Rightarrow (2|17) = 1$)~~

~~$= (17|31)$ Q.R., $17 \equiv 1 \bmod 4$~~

~~$= (-3|17)$ (reduce mod 17)~~

4. $(62|71) = (-9|71)$ reduce mod 71.

$= (-1 \cdot 3^2 | 71)$

$= (-1|71) \cdot (3^2|71)$ multiplicativity

$= (-1|71)$ $\left(\cdot (3^2|71) = 1 \right)$ as 3^2 is a square...

$= (-1)^{35} = -1$ (Euler's criterion)

Alternative approach:

$(62|71) = (2|71)(31|71)$ multiplicativity

$= 1 \cdot (31|71)$ $\left(71 \equiv \pm 1 \bmod 8 \Rightarrow (2|71) = 1 \right)$

$= -1\,(71|31)$ Q.R. $31 \equiv 71 \equiv 3 \bmod 4$.

$= -(9|31)$ reduce mod 31

$= -1$ 9 is a square.

Problem 4. ~~The only residues~~ A perfect square can only have the residue 0 or 1 modulo 4: $0^2 \equiv 0 \bmod 4$, $1^2 \equiv 1 \bmod 4$, $2^2 \equiv 0 \bmod 4$, and $3^2 \equiv 1 \bmod 4$. So if 38,948,127,483 has residue 2 or 3 mod 4, then it cannot be a perfect square. We observe

$$38{,}948{,}127{,}483 = 389481274 \cdot 100 + 80 + 3$$

$$\equiv 0 + 0 + 3 \bmod 4$$

$$\equiv 3 \bmod 4.$$

Hence 38,948,127,483 is not a perfect square. (clearly $100 \equiv 0 \bmod 4$ and $80 \equiv 0 \bmod 4$).

~~A proof~~ An argument by having the calculator approximate $\sqrt{38948127483}$ was not given much credit.

Problem 5:

We first rewrite the congruences into a standard form.

$3x \equiv 1 \pmod 7$ $\quad\rightsquigarrow\quad$ $x \equiv 5 \pmod 7$ as $5 \cdot 3 \equiv 1 \bmod 7$

$x \equiv 0 \pmod 5$ $\quad\rightsquigarrow\quad$ $x \equiv 0 \pmod 5$

$5x \equiv 1 \pmod 9$ $\quad\rightsquigarrow\quad$ $x \equiv 2 \pmod 9$ as $5 \cdot 2 \equiv 1 \bmod 9$

Method 1: We must have ~~$x=0$~~ $x = 5t$ for some $t \in \mathbb{Z}$ and

So $x = 5t \equiv 5 \bmod 7$ must hold too. Thus

$t \equiv 15 \bmod 7 \equiv 1 \bmod 7$, i.e., $t = 1 + 7s$ for $s \in \mathbb{Z}$.

Hence $x = 5(1+7s) = 5 + 5 \cdot 7 \cdot s$ for $s \in \mathbb{Z}$.

But also, we need $5 + 5 \cdot 7 \cdot s \equiv 2 \bmod 9$, that is

$$5 \cdot 7 \cdot s \equiv -3 \bmod 9$$

$$(-1) \cdot s \equiv -3 \bmod 9$$

$$s \equiv 3 \bmod 9.$$

Hence $s = 3 + 9r$ for $r \in \mathbb{Z}$. We thus conclude

$x = 5 + 5 \cdot 7 \cdot (3 + 9r) = 110 + 315r$, for all $r \in \mathbb{Z}$.

In other words, ~~the comp~~ the complete set of integer solutions is given by those x satisfying $x \equiv 110 \bmod 315$.

Method 2: (Textbook method)

$n = 5 \cdot 7 \cdot 9 = 315$

$N_1 = 63$ $\qquad N_2 = 45$ $\qquad N_3 = 35$

Also: $63x_1 \equiv 1 \bmod 5$ $\qquad 45x_2 \equiv 1 \bmod 7$ $\qquad 35x_3 \equiv 1 \bmod 9$

$3x_1 \equiv 1 \bmod 5$ $\qquad 3x_2 \equiv 1 \bmod 7$ $\qquad x_3 \equiv -1 \bmod 9$

$x_1 \equiv 2 \bmod 5$ $\qquad x_2 \equiv 5 \bmod 7$ $\qquad \equiv 8 \bmod 9$.

So a specific solution is given by

$\bar{x} = 0 \cdot 63 \cdot 2 + 5 \cdot 5 \cdot 45 + 2 \cdot 8 \cdot 35$

$= 1685$. The Chinese Remainder Theorem says every soln to the system then satisfies

$x \equiv 1685 \bmod 315 \equiv 110 \bmod 315$.

6 (1) The natural number $n=8$ does not have a primitive root.

That is, there is no integer $a \in \mathbb{Z}$, $GCD(a, 8) = 1$, for which $\phi(8) = (8-4) = 4$ is the order of a.

We can just directly verify this by checking the cases $a \in \{1, 3, 5, 7\}$.

As $1^1 \equiv 1 \bmod 8$, the order of 1 is 1.

As $3 \not\equiv 1 \bmod 8$ and $3^2 \equiv 9 \equiv 1 \bmod 8$, order of 3 is 2.

As $5 \not\equiv 1 \bmod 8$ and $5^2 \equiv 25 \equiv 1 \bmod 8$, order of 5 is 2.

As $7 \not\equiv 1 \bmod 8$ and $7^2 \equiv 49 \equiv 1 \bmod 8$, order of 7 is 2.

Thus there is no unit for 8 that has order $\phi(8)$, so $n=8$ has no primitive root.

(2) As 3 is a ~~quadr~~ primitive root of 17, the quadratic residues mod 17 are simply the numbers congruent to $3^{2k} \pmod{17}$ for $1 \le 2k \le 16$, i.e., $3^2 \equiv 9 \bmod 17$, $3^4 \equiv 13 \bmod 17$, $3^6 \equiv 15 \bmod 17$, $3^8 \equiv 16 \bmod 17$, $3^{10} \equiv 8 \bmod 17$, $3^{12} \equiv 4 \bmod 17$, $3^{14} \equiv 2 \bmod 17$, $3^{16} \equiv 1 \bmod 17$.

(It wasn't necessary to reduce mod 17 to get full credit if they justified their list adequately).

Problem 7: (1) Let p be an odd prime and suppose a is a quadratic residue for p. Then $1 = (a|p) \equiv a^{\frac{p-1}{2}} \bmod p$ by Euler's criterion. Thus the order of a is at most $\frac{p-1}{2}$, and $\frac{p-1}{2} < \phi(p) = p-1$. Hence the order of a cannot be $p-1$, so a is not a primitive root for p.

(2) We have proven in class that $(2|p) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8 \\ -1 & \text{if } p \equiv \pm 3 \bmod 8 \end{cases}$.

With this result and part (1), we see that 2 is a quadratic residue mod p when $p \equiv \pm 1 \bmod 8$, and hence 2 is not a primitive root for p.

Problem 8: We first show that when $3 \nmid n$ that $\phi(3n) = 2\phi(n)$ holds. As $3 \nmid n$, $GCD(3, n) = 1$. So we may use the multiplicativity of the Euler ϕ-function to get $\phi(3n) = \phi(3)\,\phi(n) = 2 \cdot \phi(n)$ as $\phi(3) = 3^1 - 3^0 = 2$ by the prime power formula (or check directly...)

To show the converse, we must show that if $n \in \mathbb{N}$ satisfies $\phi(3n) = 2\phi(n)$ then $3 \nmid n$. We can prove this by a proof of the contrapositive. That is, we show that if $3 \mid n$, then $\phi(3n) \neq 2\phi(n)$.

As $3 \mid n$, we may write $n = 3^k \cdot m$ for $k \geq 1$, $m \in \mathbb{N}$, $3 \nmid m$ by the Fundamental Theorem of Arithmetic. Thus $\phi(n) = \phi(3^k) \cdot \phi(m)$ by multiplicativity $= (3^k - 3^{k-1})\phi(m)$.

But now
$$\begin{aligned} \phi(3n) = \phi(3^{k+1} \cdot m) &= (3^{k+1} - 3^k)\,\phi(m) \\ &= 3 \cdot (3^k - 3^{k-1})\,\phi(m) \\ &= 3 \cdot \phi(n) \\ &\neq 2 \cdot \phi(n) \end{aligned}$$
as $\phi(n) \neq 0$ for all $n \in \mathbb{N}$. $\square$