When I refer to specific theorem numbers, they’re from the book “Elementary Number Theory” by Jones and Jones, published by Springer. I sometimes use the shorthand CRT for the Chinese Remainder Theorem. Please let me know if there are any typos or mistakes by emailing arjun-at-cims-dot-nyu-dot-edu.

**Problem 1.** This is just manual computation. The following string of numbers is the values $\phi$ takes from 1 to 16.

\[1, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4, 12, 6, 8, 8.\]

**Problem 2.** Again, this is tedious to do by hand. It’s best to use Mathematica or Wolfram alpha. Please see the attached Mathematica notebook. It can be read on the CIMS machines in the lab on the 2nd floor. One can directly view the order on Wolfram Alpha by typing

```
MulitplicativeOrder[2,9].
```

In general, you need to check that $i$ is a unit mod $n$, and the type use the command above.

**Problem 3.**

Item (a)

It’s clear that \(\text{ord}(\alpha \beta) \leq \text{ord}(\alpha)\text{ord}(\beta)\) since

\[(\alpha \beta)^{\text{ord}(\alpha)\text{ord}(\beta)} = 1.\]

In fact, (see the midterm solutions - this should be a standard argument to you by now) it’s also clear that \(\text{ord}(\alpha \beta)\text{ord}(\alpha)\text{ord}(\beta)\). Since \(\text{ord}(\alpha)\) and \(\text{ord}(\beta)\) are coprime, \(\text{ord}(\alpha \beta)\) must divide one or the other (or both). So without loss of generality, we can write

\[\text{ord}(\alpha \beta) = \frac{\text{ord}(\alpha)}{k}\text{ord}(\beta)\]

for \(k \geq 1\). Then, by definition we have

\[(\alpha \beta)^{\frac{\text{ord}(\alpha)}{k}\text{ord}(\beta)} = 1,\]

from which it follows that

\[\alpha^{\text{ord}(\alpha)} = 1.\]

Then it follows from the definition of order that \(k = 1\).

Item (b)

Again, this problem follows almost by definition. Let

\[g = \gcd(e, \text{ord}(\alpha)).\]

Since \(g|e\) and \(g|\text{ord}(\alpha)\), we can move exponents around to get that

\[(\alpha^e)^{\text{ord}(\alpha)/g} = (\alpha^{\text{ord}(\alpha)})^{e/g} = 1.\]
Hence,
\[ \text{ord}(\alpha^e) \bigg| \frac{\text{ord}(\alpha)}{g}. \]

Now we go in the opposite direction to prove \((\text{ord}(\alpha)/g) \mid \text{ord}(\alpha^e)\). Again,
\[ \alpha^{\text{ord}(\alpha^e)e} = 1 \Rightarrow \text{ord}(\alpha) \mid \text{ord}(\alpha^e)e. \]

We can divide by \(g\) to get
\[ \frac{\text{ord}(\alpha)}{g} \bigg| \frac{e}{g} \text{ord}(\alpha^e). \]

However, it’s an old theorem of ours (see Corollary 1.10 of J& J) that
\[ \gcd\left( \frac{\text{ord}(\alpha)}{g}, e \right) = 1. \]

This means that we must have \((\text{ord}(\alpha)/g) \mid \text{ord}(\alpha^e)\), and we’re done.

**Problem 4.** This is Gauss’ proof of the existence of a primitive root (PR) mod \(p\), where \(p\) is prime.

**Item (a)**
Consider the polynomial
\[ x^{(p-1)/q_i^{e_i}} - 1 \mod p. \]
All the elements of \(U_p\) (of which there are \(p-1\)) cannot be roots, since this violates Lagrange’s theorem: if the modulus \(p\) is prime, a non-zero polynomial of degree \(d\) can have at most \(d\) roots. Hence there is at least one \(\alpha_i\) that is not a root of the polynomial, and this is what we set out to prove.

**Item (b)**
For \(\alpha_i\) chosen as above, let \(\beta_i = \alpha_i^{(p-1)/q_i^{e_i}}\). Using the same argument as in the previous problem it follows (from Fermat’s theorem) that \(\text{ord}(\beta_i)|q_i^{e_i}\). Since \(q_i\) is prime,
\[ \text{ord}(\beta_i) = q_i^{e_i} \quad 0 \leq m_i \leq e_i. \]

If \(m_i\) is strictly smaller than \(e_i\); i.e., \(m_i \leq e_i - 1\) it follows that
\[ \alpha_i^{(p-1)/q_i^{e_i-m_i}} = 1 \Rightarrow \alpha_i^{(p-1)/q_i} = 1 \mod p, \]
by raising the equation to the \(q_i^{e_i-m_i-1}\)th power. But this produces a contradiction by part (a). Hence, we must have that \(\text{ord}(\beta_i) = q_i^{e_i}\).

**Item (c)**
The last part follows immediately from Problem 3(a).
\[ \text{ord}(\beta) = \text{ord}(\beta_1) \cdots \text{ord}(\beta_k) = q_1^{e_1} \cdots q_k^{e_k} = p - 1. \]

This means that we have a primitive root. Quite a neat proof, isn’t it?

**Problem 5.**

**Item (a)**
Checking each power of 2, it’s clear that 2 is a primitive root mod 5. From the proof of Theorem 6.7 in J& J, it follows that \(\text{ord}(2) = \phi(5) = 4\), or \(\text{ord}(2) = \phi(25) = 20\).

Checking
\[ 2^4 = 16 \not\equiv 1 \mod 25, \]
it follows that 2 is a primitive root. Note that if it turned out that \( \text{ord}(2) = 4 \mod 25 \), the proof of Theorem 6.7 also shows us that \( 2 + 5 = 7 \) must be a primitive root (PR).

Item (b)
We will solve

\[ x^5 = 1 \mod 5^2 \cdot 11 \]

by first solving it with respect to the moduli 25 and 11 separately, and use the Chinese Remainder Theorem (CRT) to produce a solution \( \mod 25 \cdot 11 = 275 \). For this we need PRs for both moduli: 2 is a PR mod 25 from part (a), and one can easily check that 2 is also a PR mod 11.

Since every element can be written as \( 2^i \) in \( \mathbb{U}_{25} \), we get the equation

\[ 2^{5i} = 2^0 \mod 25. \]

Since \( \phi(25) = 20 \) and 2 is a PR, \( 2^{5i} = 2^0 \iff 5i = 0 \mod 20 \). Dividing through by 5, \( i = 0 \mod 4 \). This tells us that the solution set is

\[ \{ 2^i \mid i = 0, 4, 8, 12, \text{ and } 16 \mod 20 \}. \]

Similarly, we get that the solutions mod 11 are of the form

\[ \{ 2^k \mid k = 0, 2, 4, 6, 8 \mod 10 \}. \]

Using the CRT, we know that we can always find a distinct congruence class \( x \in \mathbb{U}_{25, 11} \) such that \( x = 2^i \mod 25 \) and \( x = 2^k \mod 11 \) for each allowable pair \( i, k \). Hence we get 25 solutions mod \( 25 \cdot 11 \); they are

\[ 1, 26, 126, 251, 201, 166, 191, 16, 141, 91, 56, 81, 181, 31, 256, 221, 246, 71, 196, 146, 111, 136, 236, 86, 36. \]

**Problem 6.**

Item (a)
A moment’s thought tells you that

\[ e(n) = \max_{\alpha \in \mathbb{U}_n} \text{ord}(\alpha). \]

This means that there is an element \( g \in \mathbb{U}_n \) such that \( \text{ord}(g) = e(n) \). But we’ve proved earlier that \( \text{ord}(g)|\phi(n) \), and hence \( e(n)|\phi(n) \).

By definition, we know that there is a primitive root in \( \mathbb{U}_n \) iff there is an element with order \( \phi(n) \). From Euler’s theorem (Theorem 5.3 in J & J), it follows that \( e(n) = \phi(n) \) iff there is a primitive root.

Item (b)
Let \( \alpha \in \mathbb{U}_n \) and \( \beta \in \mathbb{U}_m \) be such that \( \text{ord}(\alpha) = e(n) \) and \( \text{ord}(\beta) = e(m) \). Since \( m \) and \( n \) are coprime, the CRT tells us that we can always find \( x \in \mathbb{U}_{mn} \) such that

\[ x = \alpha \mod n, \]
\[ x = \beta \mod m. \]

We know that

\[ x^{e(mn)} = 1 \mod mn \Leftrightarrow x^{e(mn)} = 1 \mod m \text{ and } x^{e(mn)} = 1 \mod n, \]

since \( m \) and \( n \) are coprime. Hence, \( \text{ord}(\alpha) = e(n)|e(mn) \) and \( \text{ord}(\beta) = e(m)|e(mn) \). In other words, \( e(mn) \) is a common multiple of \( e(m) \) and \( e(n) \). It’s clear that
the least such number we can pick is the lcm(e(m), e(n)), and the result follows immediately.

Item (c)
If \( n = p^e \) for an odd prime \( p \), we know that a primitive root exists. Then \( e(n) = \phi(n) \) follows from part (a).

Consider \( n = 2^e \). For \( e = 1 \), and 2, we can manually check each member of \( U_n \) to verify the result. For \( e > 2 \), most of the ideas are in Theorem 6.8 of J & J. Each element in \( U_n \) must have order \( 2^k \) for some \( k \leq \phi(2^e) = 2^{e-1} \). The proof demonstrates that all odd \( a \in \mathbb{Z}_n \) (and hence, all elements of \( U_n \)) have order at most \( 2^{e-2} \). It remains to show that there is an element with order exactly \( 2^{e-2} \). This is proved in Lemma 6.9 and Theorem 6.10 in J & J. It states that

\[
U_{2^e} = \{ \pm 5^i \mid 0 \leq i < 2^{e-2} \}.
\]

Item (d)
Using part (a), we get

\[
e(100) = e(5^2, 2^2) = \text{lcm}(e(5^2), e(2^2)) = \text{lcm}(\phi(5^2), 2^2) = \text{lcm}(20, 2) = 20.
\]

To find the last 2 digits of \( 2^{550} \), we only need to look at its value mod 100 (consider its decimal expansion). It’s easy to calculate that \( \phi(100) = \phi(2^2 5^2) = 2 \cdot 20 = 40 \).

Using this, we calculate that

\[
2^{550} = 2^{40 \cdot 13 + 30} = 2^{30} \mod 100,
\]

This doesn’t get us very far. Instead, using the exponent \( e(100) = 20 \), we get that

\[
2^{550} = 2^{20 \cdot 27 + 10} = 2^{10} = 128 \cdot (2^3) = 28 \cdot 8 = 112 \cdot 2 = 12 \cdot 2 = 24 \mod 100.
\]

**Problem 7.**

Item (a)
For \( e = 1, 2 \) we just check manually:

- \( x^2 = 1 \mod 2 \) has solution \( x = 1/2 \)
- \( x^2 = 1 \mod 4 \) has solutions \( x = 1, 3 \).

The key to solving the equation for higher powers \( e \geq 3 \) is the fact that

(1)

\[
U_{2^e} = \{ \pm 5^i \mid 0 \leq i < 2^{e-2} \},
\]

as stated in the previous problem. Then, if \( 5^i \) is a solution, so is \( -5^i \). This means that we don’t have to check too many numbers. We find that \( x = \pm 5^0, \pm 5^1 \) are solutions. That is, all members of \( U_8 \) are solutions to \( x^2 = 1 \mod 8 \). This is another illustration that Lagrange’s theorem (the one which says that a polynomial of degree \( d \) has at most \( d \) roots) holds only for prime moduli.

Item (b)
Let \( n = 2^e p_1^{e_1} \cdots p_k^{e_k} \) as stated in the problem. We’ll solve \( x^2 = 1 \mod p^e \) modulo each prime power factor of \( n \) and then combine these solutions using the Chinese Remainder Theorem. Consider

\[
x^2 = 1 \mod p^e,
\]

where \( p \) is an odd prime. We know that a primitive root exists; call the it \( \alpha \). Any element of \( U_{p^e} \) can be written as \( \alpha^i \), and hence we get

\[
\alpha^{2i} = 0 \mod p^e.
\]
We know that $\text{ord}(\alpha) = \phi(p^e) = p^e - 1(p - 1)$, and hence we must have

$$2i = 0 \mod p^e - 1(p - 1).$$

Aside: As a reminder, consider a congruence of the form

$$ax = b \mod n.$$ 

This equation, we know, has a solution iff $d = \gcd(a,n)|b$. Then, dividing through by $d$, we get

$$\frac{a}{d}x = \frac{b}{d} \mod \frac{n}{d}.$$ 

Since $\gcd(a/d, n/d) = 1$ using an old fact from chapter 1 of J & J, there must be a unique solution mod $n/d$ to this equation. This implies that $ax = b \mod n$ has $\gcd(a,b)$ distinct congruence classes of solutions.

Remark 1. For the problem at hand, we must have $\gcd(2, p^e(p - 1)) = 2$ congruence classes of solutions. This is true for each odd prime factor of $n$, and note that there are $k$ of them.

For the equation $x^2 = 1 \mod 2^e$, we get that there are 1 and 2 solutions for $e = 1$ and $e = 2$ respectively. For $e \geq 3$, we use (1) to get that

$$5^{2i} = 1 \mod 2^e \iff 2i = 0 \mod 2^{e-2},$$

using the fact that $\text{ord}(5) = 2^{e-2}$. This gives us two solutions of the form $5^i$. The same argument can be repeated for elements in $U_{2^e}$ of the form $-5^i$, to get two more solutions for a total of 4. Combining the discussion in this paragraph and Remark 1, we can use the CRT (or more precisely, Theorem 3.11 in J & J) to get that the number of solutions mod $n$ is

$$2^k \quad \text{for } e = 1,$$

$$2^{k+1} \quad \text{for } e = 2,$$

$$2^{k+2} \quad \text{for } e \geq 3.$$ 

Remark 2. The important observation here is that $f(n)$, the number of solutions to $x^2 = 1 \mod n$, gives the number of elements of $U_n$ that are their own inverses.

Item (c)

Notice that the number of roots of $x^2 - 1 \mod n$ is 2 if either $k = 1, e = 0$, or $k = 0, e = 1$. This means that $n = 2$ or $n = p^e$ for some prime $p$. In particular, $f(p) = 2$ for each prime $p$, and the fact that

$$\prod_{u \in U_n} u = -1 \mod n$$

is just Wilson’s theorem. The proof of Wilson’s theorem in the textbook is not very illuminating in the context of this problem. Let’s try to figure out what’s really going on.

Let the elements of $U_n$ be $\{u_1, \ldots, u_{\phi(n)}\}$. Consider the product

$$P = u_1 \cdots u_{\phi(n)}.$$ 

By Remark 2, we can pair up elements that are not their own inverses in the product $P$; i.e., for each element $u_i$ such that $u_i^2 \neq 1$, we can find a unique $u_j$ such that
$u_i u_j = 1$. We can combine such $u_i$ in $P$, and relabel the rest of the elements so that we’re left with the $f(n)$ roots of $x^2 = 1$:

$$P = u_1 \cdots u_{f(n)}.$$ 

Now, if $u_1$ is a root of $x^2 - 1$, so is $-u_1$. We rewrite $P$ again to get

$$P = u_1 (-u_1) \cdots u_{f(n)/2} (-u_{f(n)/2}) = (-1)^{f(n)/2},$$

and the result follows immediately.

**Problem 8.** The solutions are in J & J: see Lemma 4.8 and Theorem 6.15.