18.781 Practice Questions for Midterm 2

Note: The actual exam will be shorter (about 10 of these questions), in case you are timing yourself.

1. Find a primitive root modulo $343 = 7^3$.

   Solution: We start with a primitive root modulo 7, for example 3. The proof of existence of primitive roots modulo p^2 shows that if g is a primitive root mod p, then there is exactly one value of t mod p such that $g + tp$ is *not* a primitive root mod p^2, and for this value of t, we will have $(g + tp)^{p-1} \equiv 1 \pmod{p^2}$. So we just compute 3^6 modulo 49, and see that we get $43 \not\equiv 1 \pmod{49}$. Therefore, 3 is a primitive root modulo 49. Now the proof of existence of primitive roots modulo p^e showed that if we have a primitive root mod p^2, it's also a primitive root mod p^e. So 3 is a primitive root modulo 343 as well.

2. How many solutions are there to $x^{12} \equiv 7 \pmod{19}$? To $x^{12} \equiv 6 \pmod{19}$?

   Solution: In general, if $p \nmid a$, the number of solutions to $x^k \equiv a \pmod{p}$ can be calculated as follows. Let $d = \gcd(k, p-1)$. Then there are no solutions if $a^{(p-1)/d} \not\equiv 1 \pmod{p}$, and there are d solutions if $a^{(p-1)/d} \equiv 1 \pmod{p}$. To see this, let g be a primitive root mod p. Write $a = g^b$. Then any x solving the congruence equals g^m for some m, and then the congruence says $g^{mk} \equiv g^b \pmod{p}$, which is equivalent to $mk \equiv b \pmod{p-1}$, since the order of g mod p is $p - 1$. Now this is just a linear congruence, and it has exactly 0 or $d = \gcd(k, p-1)$ solutions, according to whether $d \nmid b$ or $d|b$. This latter condition is equivalent to whether or not $p - 1$ divides $(p - 1)b/d$, which is equivalent to whether $1 \equiv g^{(p-1)b/d} = a^{(p-1)/d} \pmod{p}$.

   For the given examples, compute $7^{18/6} = 7^3 \equiv 1 \pmod{19}$, so the first congruence has 6 solutions. On the other hand, $6^3 \equiv 7 \pmod{19}$, so the second congruence has no solutions.

3. Solve the congruence $3x^2 + 4x - 2 \equiv 0 \pmod{31}$. **Solution:** First, we make the congruence monic by inverting 3 mod 31. Noting that $3 \cdot 10 = 30 \equiv -1 \pmod{31}$, we see that $3^{-1} = -10$. So

   $$x^2 - 40x + 20 \equiv 0 \pmod{31}.$$

   Next, complete the square to see

   $$(x - 20)^2 \equiv 20^2 - 20 = 380 \equiv 8 \pmod{31}.$$

   We need to check whether 8 is a square mod 31 and also to compute a square root if it is. First, check

   $$\left(\frac{8}{31}\right) = \left(\frac{2}{31}\right) = 1.$$

   To compute a square root, one can use Tonelli's algorithm. Here, it's pretty easy since $31 \equiv 3 \pmod{4}$. So a square root of 8 is

   $$8^{(31+1)/4} = 8^8 = 2^{24} \equiv 16 \pmod{31}.$$

   So $x \equiv 20 \pm 16 \pmod{31}$. i.e $x \equiv 4, 5 \pmod{31}$ are the two solutions.

4. Characterize all primes p such that 15 is a square modulo p.

Solution: Obviously 15 is a square mod $2, 3, 5$. So suppose $p > 5$. We compute the Jacobi symbol

$$\left(\frac{15}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{5}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)\left(\frac{p}{5}\right).$$

So the answer will depend on p modulo $4 \cdot 15 = 60$. Looking at the $\phi(60) = 2 \cdot 2 \cdot 4 = 16$ residue classes mod 60, we see that the RHS is $+1$ exactly when

$$p \equiv \pm 1, \pm 7, \pm 11, \pm 17 \pmod{60}.$$

5. If n is odd, evaluate the Jacobi symbol $\left(\frac{n^3}{n-2}\right)$.

Solution: Using quadratic reciprocity for the Jacobi symbol (noting that one of n and $n-2$ must be 1 mod 4, we have

$$\left(\frac{n^3}{n-2}\right) = \left(\frac{n}{n-2}\right) = \left(\frac{n-2}{n}\right) = \left(\frac{-2}{n}\right)$$

which is 1 when $n \equiv 1, 3 \pmod 8$ and -1 when $n \equiv 5, 7 \pmod 8$.

6. If $n = p_1^{e_1} \dots p_r^{e_r}$, how many squares modulo n are there? How many quadratic residues modulo n are there (i.e. the squares which are coprime to n)?

Solution: For both these questions, we can use the Chinese Remainder theorem. Let's solve the second question first. If p is an odd prime, then there are $(p-1)/2$ quadratic residues mod p. For each such quadratic residue a, Hensel's lemma can be applied to $f(x) = x^2 - a$ to see that a (and anything congruent to a mod p^e) must be a square. Since there are p^{e-1} such lifts for every choice of $a \not\equiv 0 \pmod p$, we see that the number of quadratic residues mod p^e is $p^{e-1}(p-1)/2 = p^e(1-1/p) \cdot 1/2$. If $p = 2$, then we can use the fact that modulo $2, 4, 8$ there is exactly one quadratic residue (namely 1), and if a is a square mod 8, then it is a square mod every higher power of 2 (this follows from an extended version of Hensel's lemma). So the number of quadratic residues mod 2^e is : 1 if $e \le 3$ and 2^{e-3} if $e > 3$. Therefore, the number of quadratic residues mod $n = 2^e \prod p_i^{e_i}$ is, by CRT, equal to

$$\max(1, 2^{e-3}) \prod p_i^{e_i - 1}(p_i - 1)/2.$$

Now for the number of squares mod n. The number of squares will again be a product over all the primes dividing n, of the number of squares mod $p_i^{e_i}$. Separate out the squares according to what their gcd with p^e is; it must be an even power of p. We get the following: if e is even then

$$p^{e-1} \cdot \frac{p-1}{2} + p^{e-3} \cdot \frac{p-1}{2} + \cdots + p \cdot \frac{p-1}{2} + 1$$

(the last term corresponding to 0 being a square mod p^e). The sum equals

$$\begin{aligned}\frac{p^{e-1}(p-1)}{2}(1 + p^{-2} + \cdots + p^{-2(e/2-1)}) + 1 &= \frac{p^{e-1}(p-1)}{2} \cdot \frac{(1-p^{-e})}{1-p^{-2}} + 1 \\ &= \frac{p(p^e-1)}{2(p+1)} + 1 = \frac{p(p^e+1)+2}{2(p+1)}.\end{aligned}$$

Similarly, if e is odd we get

$$p^{e-1}\cdot\frac{p-1}{2}+p^{e-3}\cdot\frac{p-1}{2}+\cdots+\cdot\frac{p-1}{2}+1=\frac{p^{e+1}+2p+1}{2(p+1)}.$$

I'll leave the calculation for when $p=2$ to you. The answer is

$$\frac{2^{e-1}+4}{3} \text{ if } e \text{ is even }, \quad \frac{2^{e-1}+5}{3} \text{ if } e \text{ is odd.}$$

7. Let $p>3$ be a prime. Show that the number of solutions (x,y) of the congruence $x^2+y^2\equiv 3 \pmod{p}$ is $p-\left(\frac{-1}{p}\right)$.

8. The number of solutions is

$$\sum_{x=0}^{p-1}\left(\left(\frac{3-x^2}{p}\right)+1\right)=p+\sum_{x=0}^{p-1}\left(\frac{3-x^2}{p}\right)=p+\sum_{x=0}^{p-1}\left(\frac{-1}{p}\right)\left(\frac{x^2-3}{p}\right)$$
$$=p+\left(\frac{-1}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^2-3}{p}\right)$$

We showed on homework that for any k, $\sum\left(\frac{x^2+k}{p}\right)=-1$. Therefore the expression above simplifies to $p-\left(\frac{-1}{p}\right)$.

9. Compute (with justification) the cyclotomic polynomial $\Phi_{12}(x)$.

Solution: We start with $x^{12}-1$, factoring it and removing any factors that divide x^d-1 for proper divisors d of 12. We have

$$x^{12}-1=(x^6-1)(x^6+1)$$

and so we can immediately throw out x^6-1. Next,

$$x^6+1=(x^2+1)(x^4-x^2+1)$$

and x^2+1 is a factor of x^4-1. So $\Phi_{12}(x)$ must divide x^4-x^2+1. Now since $\phi(12)=4$, we see that equality must hold. So $\Phi_{12}(x)=x^4-x^2+1$.

10. Let $f(n)=(-1)^n$. Compute

$$Z(f,2)=\sum_{n\geq 1}\frac{f(n)}{n^2}.$$

(you may use that $\sum 1/n^2=\pi^2/6$.)

Solution: We want to know the value of

$$S=-1+\frac{1}{2^2}-\frac{1}{3^2}+\frac{1}{4^2}-\frac{1}{5^2}+\ldots$$

We already know

$$\frac{\pi^2}{6} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \dots$$

Adding these we get

$$\begin{aligned} S + \frac{\pi^2}{6} &= 2\left(\frac{1}{2^2} + \frac{1}{4^2} + \frac{1}{6^2} + \dots\right) \\ &= 2 \cdot \frac{1}{4} \cdot \left(\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots\right) \\ &= 2 \cdot \frac{1}{4} \cdot \frac{\pi^2}{6}. \end{aligned}$$

Therefore $S = -\pi^2/12$.

11. For $n = p_1^{e_1} \dots p_r^{e_r}$, calculate the value of $(U * U * U)(n)$, where U is the arithmetic function such that $U(n) = 1$ for all n.

    Solution: Since U is multiplicative, so is $U * U * U$. So enough to calculate it for p^e. Then we have

    $$(U * U * U)(p^e) = \sum_{d_1 d_2 d_3 = p^e} U(d_1)U(d_2)U(d_3) = \sum_{e_1+e_2+e_3=e} 1$$

    since d_i can only be a power of p, say p^{e_i}. So the value of the function is just the number of nonnegative integer solutions of $e_1 + e_2 + e_3 = e$. There are many ways to compute this number. One easy way is: if we fix any e_1 between 0 and e, the number of possible e_2 is $e - e_1 + 1$ (since e_2 can range between 0 and $e - e_1$) and then e_3 is forced to equal $e - e_1 - e_2$. So the total number of solutions is

    $$\sum_{e_1=0}^{e} (e - e_1 + 1) = \sum_{e_1=0}^{e} (e+1) - \sum_{e_1=0}^{e} e_1 = (e+1)^2 - e(e+1)/2 = (e+1)(e+2)/2.$$

    So for $n = p_1^{e_1} \dots p_r^{e_r}$, by multiplicativity, we have

    $$(U * U * U)(n) = \prod_{i=1}^{r} (e_i + 1)(e_i + 2)/2.$$

12. Let p be a prime which is 1 mod 4, and suppose $p = a^2 + b^2$ with a odd and positive. Show that $\left(\frac{a}{p}\right) = 1$.

    Solution: We have by Quadratic Reciprocity,

    $$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{a^2+b^2}{a}\right) = \left(\frac{b^2}{a}\right) = 1.$$

13. Let a_1, a_2, a_3, a_4 be integers. Show that the product $p = \prod_{i<j}(a_i - a_j)$ is divisible by 12.

    Solution: Enough to show it's divisible by 3 and by 4. Since there are four integers, and only three residue classes mod 3, two of them must be congruent mod 3. Therefore divisibility by 3 follows. For divisibility by 4, note that the only way no two of them are congruent modulo 4 is if they are all the four distinct classes mod 4, namely $0, 1, 2, 3$. But then $0 - 2$ and $1 - 3$ are both divisible by 2, which makes the product divisible by $2^2 = 4$.

14. Let the sequence $\{a_n\}$ be given by $a_0 = 0, a_1 = 1$ and for $n \geq 2$,

$$a_n = 5a_{n-1} - 6a_{n-2}.$$

Show that for every prime $p > 3$, we have $p \mid a_{p-1}$.

Solution: The characteristic polynomial is $T^2 - 5T + 6 = (T-2)(T-3)$. So we must have $a_n = A \cdot 3^n + B \cdot 2^n$ for some A, B. Plugging in $n = 0, 1$ we get $A = 1, B = -1$. So $a_n = 3^n - 2^n$. Now by Fermat, if $p > 3$ then $2^{p-1} \equiv 1 \equiv 3^{p-1} \pmod{p}$, so $a_{p-1} \equiv 0 \pmod{p}$.

15. Find a positive integer such that $\mu(n) + \mu(n+1) + \mu(n+2) = 3$.

Solution: We know $\mu(n) = \pm 1$ if n is squarefree, and 0 otherwise. The only way we could have the equation holding is if $\mu(n) = \mu(n+1) = \mu(n+2) = 1$. That is, $n, n+1, n+2$ are all squarefree and products of an even number of primes. In particular, n must be 1 mod 4 (else 4 will divide one of these numbers). Trying the first few values, we see that $n = 33$ is the smallest value which works.

16. Compute the set of integers n for which $\sum_{d|n} \mu(d)\phi(d) = 0$.

Solution: Since $\mu(n)\phi(n)$ is a multiplicative function of n, so is

$$f(n) = \sum_{d|n} \mu(d)\phi(d).$$

Let's compute what it is on prime powers. We have $f(1) = 1$, and for $e \geq 1$, $f(p^e) = \phi(1) - \phi(p) = 2 - p$. Therefore, for $n = p_1^{e_1} \dots p_r^{e_r}$, we have $f(n) = \prod(2 - p_i)$. Therefore $f(n) = 0$ iff one of the p_i is 2, i.e. iff n is even.

17. Let f be a multiplicative function which is not identically zero. Show that $f(1) = 1$.

Solution: We have $f(1) = f(1^2) = f(1)f(1)$, so $f(1)(f(1) - 1) = 0$. If $f(1) \neq 1$, this forces $f(1) = 0$. Then $f(n) = f(n \cdot 1) = f(n)f(1) = f(n) \cdot 0 = 0$ for all n, so f is identically 0. We used that 1 is coprime to all integers.