18.781: Solution to Practice Questions for Final Exam

1. Find three solutions in positive integers of $|x^2 - 6y^2| = 1$ by first calculating the continued fraction expansion of $\sqrt{6}$.

   Solution: We have

$$\begin{aligned}
\sqrt{6} &= [2, \frac{1}{\sqrt{6}-2}] \\
&= [2, \frac{\sqrt{6}+2}{2}] \\
&= [2, 2, \frac{1}{\frac{\sqrt{6}-2}{2}}] = [2, 2, \frac{2}{\sqrt{6}-2}] = [2, 2, \sqrt{6}+2] \\
&= [2, 2, 4, \frac{1}{\sqrt{6}-2}] \\
&= [2, 2, 4, 2, 4, 2, 4, \dots] = [2, \overline{2, 4}].
\end{aligned}$$

   Therefore, looking at $[2, 2]$ we get $5/2$, which leads to $5^2 - 6 \cdot 2^2 = 1$. Therefore $(5, 2)$ is a solution. To get two more we compute

$$\begin{aligned}
(5 + 2\sqrt{6})^2 &= 49 + 20\sqrt{6} \\
(5 + 2\sqrt{6})^3 &= (5 + 2\sqrt{6}) \cdot (49 + 20\sqrt{6}) = 485 + 198\sqrt{6}.
\end{aligned}$$

   Therefore $(5, 2), (49, 20)$ and $(485, 198)$ are three solutions. Note that since the length of the period is 2 (even) there are no solutions to $x^2 - 6y^2 = -1$.

2. If $\theta_1 = [3, 1, 5, 9, a_1, a_2, \dots]$ and $\theta_2 = [3, 1, 5, 7, b_1, b_2, \dots]$, show that $|\theta_1 - \theta_2| < 49/7095$.

   Solution: Let $\theta = [3, 1, 5] = 23/6$. Then computing the next convergent to $[3, 1, 5, 9] = 211/56$, we see that $|\theta_1 - \theta| < 1/(6 \cdot 55)$. Similarly $|\theta_2 - \theta| < 1/(6 \cdot 43)$. So by the triangle inequality

$$|\theta_1 - \theta_2| \le |\theta_1 - \theta| + |\theta - \theta_2| < 1/(6 \cdot 55) + 1/(6 \cdot 43) = 49/7095.$$

   Note: once you compute $[3, 1] = 4/1$ and $[3, 1, 5] = 23/6$, you can be a bit lazy and not compute say $[3, 1, 5, 9]$, since you're only interested in $q_3 = a_3 q_2 + q_1 = 9 \cdot 6 + 1 = 55$. Similarly for $[3, 1, 5, 7]$.

3. For $n = 1728$, figure out the number of positive divisors of n, and the sum of its positive divisors.

   Solution: $n = 2^6 3^3$, so $d(n) = (6 + 1)(3 + 1) = 28$, and

$$\sigma(n) = \frac{2^7 - 1}{2 - 1} \cdot \frac{3^4 - 1}{3 - 1} = 127 \cdot 40 = 5080.$$

4. Use multiplicativity to calculate the sum

$$\sum_{d|2592} \frac{\phi(d)}{d}.$$

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

$$g = U * f = \sum_{d|n} \frac{\phi(d)}{d}.$$

So we need to figure out what it is on prime powers. We have $g(1) = 1$ and for $e \geq 1$,

$$g(p^e) = 1 + \frac{p-1}{p} + \frac{p(p-1)}{p^2} + \cdots + \frac{p^{e-1}(p-1)}{p-1} = 1 + e\left(1 - \frac{1}{p}\right).$$

Now $2592 = 2^5 3^4$. We have $g(2^5) = 1 + 5/2 = 7/2$ and $g(3^4) = 1 + 8/3 = 11/3$. So $g(n) = 77/6$.

5. Prove that if a prime $p > 3$ divides $n^2 - n + 1$ for an integer n, then $p \equiv 1 \pmod 6$. (the original problem should have said $p > 3$)

   Solution: We have $n^2 - n + 1 \equiv 0 \pmod p$. So $4n^2 - 4n + 4 \equiv 0 \pmod p$. That is, $(2n-1)^2 \equiv -3 \pmod p$. So -3 is a quadratic residue mod p (since $\gcd(3, p) = 1$). This forces $p \equiv 1 \pmod 3$, since

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

   and the last expression is $+1$ if $p \equiv 1 \pmod 3$ and -1 if $p \equiv 2 \pmod 3$.

6. Compute the value of the infinite periodic fraction $\langle 12, \overline{24} \rangle$. Find the smallest positive (i.e. both $x, y > 0$) solution of $x^2 - 145y^2 = 1$.

   Solution: Let $y = [\overline{24}] = 24 + 1/y$. Then $y^2 - 24y - 1 = 0$, so $y = 12 + \sqrt{145}$ (plus sign because $y > 0$). Therefore $x = [12, \overline{24}] = 12 + 1/y = 12 + 1/(12 + \sqrt{145}) = 12 + \sqrt{145} - 12 = \sqrt{145}$.

   The period is odd. Therefore the smallest positive solution to the Brahmagupta-Pell equation will come from $[12, 24] = 12 + 12/24 = 289/24$, and it is $(289, 24)$. Note that $[12] = 12/1$ will give $12^2 - 145 \cdot 1^2 = -1$.

7. Determine whether there is a nontrivial integer solution of the equation

   $$49x^2 + 5y^2 + 38z^2 - 28xy + 70xz - 28yz = 0.$$

   Solution: Let's simplify the conic. It's expeditious to first scale x by $1/7$, gettting

   $$x^2 + 5y^2 + 38z^2 - 4xy + 10xz - 28yz = (x - 2y + 5z)^2 + y^2 + 13z^2 - 8yz.$$

   Therefore replacing calling $(x - 2y + 5z)$ our new variable x, we get

   $$x^2 + y^2 + 13z^2 - 8yz = x^2 + (y - 4z)^2 - 3z^2.$$

   So we end up with

   $$x^2 + y^2 - 3z^2$$

   which is already nice and squarefree. By Legendre's theorem, we just need to verify whether the local conditions are satisfied. The coefficients $1, 1, -3$ don't all have the same sign, so that one's ok. We also need to check that -1 is a square mod 3, which is not ok. So the original conic doesn't have any nontrivial rational or integer points.

8. Find a Pythagorean triangle such that the difference of the two (shorter) sides is 1, and every side is at least 100.

   Solution: Suppose that the sides are $r^2 - s^2, 2rs, r^2 + s^2$. (In general, they will be some common multiple of these, but the fact that the difference of two of the sides is 1, and positivity of the sides, forces that multiple to be 1 anyway). So we need $|r^2 - s^2 - 2rs| = 1$, i.e. $|(r-s)^2 - 2s^2| = 1$. Let $x = r - s$ and $y = s$, then this is just a Brahmagupta-Pell type equation

$$x^2 - 2y^2 = \pm 1.$$

   We want a solution such that $s = y$ and $r = x+y$ are both positive, and such that $\min(2rs, r^2 - s^2)$ is larger than 100. The continued fraction of $\sqrt{2}$ is $[1, \overline{2}]$. So the smallest positive solution comes from $[1] = 1/1$, i.e. is $(x, y) = (1, 1)$ (which we could have guessed anyway, without using continued fractions). Now $1^2 - 2 \cdot 1^2 = -1$. To get all solutions, we just have to look at the rational and irrational parts of $(1+\sqrt{2})^n$. The smallest one which works is $(1+\sqrt{2})^3 = 7+5\sqrt{2}$. So we get $(r, s) = (12, 5)$. So the Pythagorean triangle is $(119, 120, 169)$.

9. Show that $x^2 + 2y^2 = 8z + 5$ has no integral solution.

   Solution: Looking mod 8, we see that we have $x^2 + 2y^2 \equiv 5 \pmod 8$. Now, further looking mod 2 we see x must be odd. So $x^2 \equiv 1 \pmod 8$, which forces $2y^2 \equiv 4 \pmod 8$. This is impossible, since if y is even, then $2y^2 \equiv 0 \pmod 8$, and if y is odd, then $2y^2 \equiv 2 \pmod 8$.

10. Define a sequence by $a_0 = 2$, $a_1 = 5$ and $a_n = 5a_{n-1} - 4a_{n-2}$ for $n \geq 2$. Show that $a_n a_{n+2} - a_{n+1}^2$ is a square for every $n \geq 0$.

    Solution: The characteristic polynomial is $T^2 - 5T + 4 = (T-1)(T-4)$. So we must have $a_n = A \cdot 4^n + B \cdot 1^n$. Subsituting in $n = 0$ and 1, we get $a_n = 4^n + 1$. So

$$\begin{aligned} a_n a_{n+2} - a_{n+1}^2 &= (4^n + 1)(4^{n+2} + 1) - (4^{n+1} + 1)^2 \\ &= 4^{n+2} + 4^n - 2 \cdot 4^{n+1} \\ &= 4^n(16 + 1 - 2 \cdot 4) = 9 \cdot 4^n = (2 \cdot 3^n)^2 \end{aligned}$$

    which is a perfect square.

11. Let $p \nmid ab$. Show that $ax^2 + by^2 \equiv c \pmod p$ has a solution.

    Solution: Consider the $(p+1)/2$ number ax^2 for $x = 0, \ldots, (p-1)/2$. These are all distinct modulo p. Similarly, the $(p+1)/2$ numbers $c - by^2$ are also all distinct modulo p. Since we now have $p+1$ numbers in all, and only p residue classes mod p, by the Pigeonhole principle, two of these must be congruent mod p. Therefore we must have $ax^2 \equiv c - by^2 \pmod p$ for some x, y. Therefore the congruence has a solution.

12. How many solutions are there to $x^2 + 3x + 18 \equiv 0 \pmod{28}$? Find all of them.

    Solution: We need to figure out the number of solutions mod 4 and mod 7, and multiply. Modulo 4 we have $x^2 + 3x + 2 \equiv (x+1)(x+2) \pmod 4$. It's easy to see this has the solutions $x \equiv -1, -2 \pmod 4$.

    Note: one must be very careful when dealing with congruences modulo prime powers. It's not necessarily true that if you have a product of (e.g. linear) factors, that the product will be zero mod p^e iff one of them is. For example, $x(x+2) \equiv 0 \pmod 8$ has more than the two solutions $x \equiv 0, -2$; in fact, any even number x will make $x(x+2)$ vanish mod 8, so there are 4 solutions mod 8. If p^e is small enough, the best strategy is probably just to run over all the congruence classes and check. On the other hand, if you're working mod a prime (i.e. $e = 1$) then you can separate out factors.

Modulo 7 we have $x^3 + 3x + 18 \equiv x^2 - 4x + 4 = (x-2)^2 \equiv 0 \pmod 7$. So just one solution $x \equiv 2 \pmod 7$. So the total number of solutions mod 28 is $2 \cdot 1 = 2$. To find them, we need the linear combination

$$2 \cdot 4 + (-1) \cdot 7 = 1.$$

Then to combine -1 and 2 we have $(-1) \cdot (-1) \cdot 7 + 2 \cdot 2 \cdot 4 = 23$. To combine -2 and 2 we have $(-2) \cdot (-1) \cdot 7 + 2 \cdot 2 \cdot 4 = 30 \equiv 2 \pmod{28}$. So the two solutions mod 28 are 2 and 23.

13. Let a, m be positive integers, not necessarily coprime. Show that $a^m \equiv a^{m-\phi(m)} \pmod m$.

    Solution: Write $m = \prod p_i^{e_i}$. Enough to prove that

    $$a^m \equiv a^{m-\phi(m)} \pmod{p_i^{e_i}}$$

    for every i. If $p_i \nmid a$ then by Euler

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

    Since $\phi(p_i^{e_i})$ divides $\phi(m) = \prod \phi(p_i^{e_i})$, we get that

    $$a^{\phi(m)} \equiv 1 \pmod{p_i^{e_i}},$$

    and then by multiplying by $a^{m-\phi(m)}$, we get the desired congruence. On the other hand, if $p_i | a$, then the left and right sides of the congruence we wish to prove will be divisible by p_i^m and $p_i^{m-\phi(m)}$ respectively. If we prove that both the exponents are at least e_i, then both sides will be congruent to 0 modulo $p_i^{e_i}$, and we'll be done. It's obviously enough to prove $m - \phi(m) \geq e_i$, since $m \geq m - \phi(m)$. We'll assume $m > 1$, since if $m = 1$ there are no primes dividing it, and nothing to prove. Now note that $m > \phi(m)$ (since $\phi(m)$ is the number of integers in $\{1, \ldots, m\}$ coprime to m, and there's at least one which is not coprime to m, namely m). Also, since $p_i^{e_i} | m$, remembering that $\phi(m) = p_i^{e_i - 1}$ times other stuff, we see that $p_i^{e_i-1}$ divides $m - \phi(m)$. So $m - \phi(m) \geq p_i^{e_i-1} \geq 2^{e_i-1} \geq e_i$ whenever $e_i \geq 1$. (It's an easy exercise to prove by induction that $2^{e-1} \geq e$ for any $e \in \mathbb{N}$.)

14. Parametrize all the rational points on the curve $x^2 - 3y^2 = 1$.

    Solution: We find one trivial point $(1, 0)$. So write $y = m(x-1)$ and plug it in, to get

    $$x^2 - 3m^2(x-1)^2 = 1$$

    So

    $$(x-1)(x+1) = 3m^2(x-1)^2.$$

    Cancelling a factor of $(x-1)$, we get

    $$x + 1 = 3m^2(x-1)$$

So $x = (3m^2+1)/(3m^2-1)$ and then $y = m(x-1) = 2m/(3m^2-1)$. This parametrizes all rational points on the conic (except for the original point $(1,0)$, which is obtained as a limit when $m \to \infty$).

15. Find an integer solution of $37x + 41y = -3$.

    Solution: We run the Euclidean algorithm on 37 and 41 to get

$$\begin{array}{rrrr} & 1 & 0 & 41 \\ & 0 & 1 & 37 \\ -1 & 1 & -1 & 4 \\ -9 & -9 & 10 & 1 \end{array}$$

    So $(-9) \cdot 41 + 10 \cdot 37 = 1$.

16. Show that if $n > 1$ then $n \nmid 2^n - 1$. (Hint: consider the smallest prime dividing n).

    Solution: By contradiction. Suppose $n | 2^n - 1$. Let p be the smallest prime dividing n. Then $p | 2^n - 1$. So the order of 2 mod p divides n. But it also divides $p - 1$. So the order h of 2 mod p is less than p and divides n, and so are the primes dividing h. Since there's no prime smaller than p which divides n, the order must be 1. So $2^1 \equiv 1 \pmod{p}$, which is impossible.

17. Let $p \geq 11$ be prime. Show that for some $n \in \{1, \ldots, 9\}$, both n and $n+1$ are quadratic residues.

    If either 2 or 5 is a quadratic residue mod p, we're done, considering the pairs $(1,2)$ and $(4,5)$, since 1 and 4 are squares and therefore quadratic residues. If both 2 and 5 are quadratic nonresidues, then 10 is a quadratic residue. So $(9,10)$ does the job.

18. Show that if $23a^2 \equiv b^2 \pmod{17}$ then $23a^2 \equiv b^2 \pmod{289}$.

    Solution: We calculate

$$\left(\frac{23}{17}\right) = \left(\frac{6}{17}\right) = \left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

    So if $23a^2 \equiv b^2 \pmod{17}$ then we claim $17 \mid a$, else we would have

$$23 \equiv (ba^{-1})^2 \pmod{17}$$

    which is a contradiction to the above calculation. So $17^2 \mid 23a^2 = b^2$ and so $17 \mid b$. Then $17^2 \mid 23a^2 - b^2$, so $23a^2 \equiv b^2 \pmod{289}$.

19. Calculate the product $\prod_\alpha (2 - \alpha)$, where α runs over the primitive 14'th roots of unity.

    Solution: We compute the cyclotomic polynomial $\Phi_{14}(x)$ noting that it must have degree $\phi(14) = 6$.

$$x^{14} - 1 = (x^7 - 1)(x^7 + 1).$$

    Throwing out $x^7 - 1$, we have

$$x^7 + 1 = (x+1)(x^6 - x^5 + x^4 - x^3 + x^2 - x + 1)$$

So

$$\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1.$$

Note that $\Phi_{14}(x) = \prod_\alpha (x - \alpha)$, where α runs over the primitive 14'th roots of unity. Substituting $x = 2$ in, we get

$$\prod_\alpha (2 - \alpha) = 2^6 - 2^5 + 2^4 - 2^3 + 2^2 - 2 + 1 = 43.$$

20. Let f be a multiplicative function with $f(1) = 1$, and let f^{-1} be its inverse for Dirichlet convolution. Show that f^{-1} is multiplicative as well, and that for squarefree n, we have $f^{-1}(n) = \mu(n)f(n)$.

Solution: The inverse f^{-1} is defined by $f * f^{-1} = \mathbf{1}$, and it exists as long as $f(1) \neq 0$, as we showed on a problem set. To show it's multiplicative, we will define a function g which will be multiplicative by definition, and show that $f * g = 1$. Then it will follow that $f^{-1} = g$. So let $g(1) = 1$, and define g on prime powers p^e by induction on $e \geq 1$ by letting

$$\begin{aligned}\mathbf{1}(p^e) = 0 = (f * g)(p^e) &= f(1)g(p^e) + f(p)g(p^{e-1}) + \dots f(p^{e-1})g(e) + f(p^e)g(1) \\ &= g(p^e) + f(p)g(p^{e-1}) + \dots f(p^{e-1})g(e) + f(p^e)g(1).\end{aligned}$$

Since $g(1), \dots, g(p^{e-1})$ have been defined by the induction hypothesis, we can solve this uniquely for $g(p^e)$. Then for $n = p_1^{e_1} \dots p_r^{e_r}$, define $g(n) = \prod g(p_i^{e_i})$. By construction, g is multiplicative. Therefore so is $g * f$. By construction $(g * f)(1) = 1$ and $(g * f)(p^e) = 0$ for $e \geq 1$. So $(g * f)(n) = 0$ for $n \geq 1$ by multiplicativity. That is, $g * f = \mathbf{1}$. Therefore g is the multiplicative inverse of f. Note that there is a unique multiplicative inverse, since if g' were another inverse, then

$$g = g * \mathbf{1} = g * (f * g') = (g * f) * g' = \mathbf{1} * g' = g'.$$

Finally, we need to show $g(n) = \mu(n)f(n)$ for n squarefree. By multiplicativity of g, μ and f, it's enough to show this when $n = p$, a prime (it's clearly true for $n = 1$). But then $g(p)$ is defined by

$$0 = g(p) + f(p)g(1) = g(p) + f(p).$$

That is, $g(p) = -f(p) = \mu(p)f(p)$, which finishes the proof.

MIT OpenCourseWare
http://ocw.mit.edu

18.781 Theory of Numbers
Spring 2012

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.