Practice Final Solutions

1. True or false:

   (a) If a is a sum of three squares, and b is a sum of three squares, then so is ab.

   False: Consider $a = 14$, $b = 2$.

   (b) No number of the form $4^m(8n + 7)$ can be written as a sum of two squares.

   True: Since it cannot be written as a sum of three squares, it cannot be written as a sum of two squares.

   (c) A number can be both a quadratic residue modulo an odd prime p, and a primitive root modulo p.

   False: If a is a quadratic residue mod p then by Euler's criterion $a^{(p-1)/2} = 1$ and so the order of a is not $p - 1$.

   (d) A perfect number must have at least four divisors.

   True: If $n > 1$ is perfect then $\sigma(n) = 2n$. If it has just two divisors then $\sigma(n) = n + 1 < 2n$. Hence it must have a third divisor d and thus also a fourth divisor n/d (which may be d and then you can argue why there must then be yet another divisor).

   (e) An infinite simple continued fraction never converges to a rational number.

   True: proved in class.

2. Let p be an odd prime. Find a formula for the Legendre symbol

$$\left(\frac{-2}{p}\right)$$

SOLUTION: One has

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$$

Let us find a formula for when this is equal to 1. The two cases are $1 \cdot 1 = 1$ and $(-1) \cdot (-1) = 1$. The first is the case if $p \equiv 1 \mod 4$ and $p \equiv \pm 1 \mod 8$. This means that one needs $p \equiv 1 \mod 8$. The second is the case if $p \equiv 3 \mod 4$ and $p \equiv 3$ or $5 \mod 8$. This means that $p \equiv 3 \mod 8$. Hence

$$\left(\frac{-2}{p}\right) = 1$$

if and only if $p \equiv 1$ or $3 \mod 8$.

3. Let $p \equiv 1 \mod 4$ be a prime and a a quadratic residue mod p. Decide with justification if then automatically $p - a$ is quadratic residue mod p.

   SOLUTION: Since $p - a \equiv -a \mod p$ it suffices to decide if $-a$ is a quadratic residue. But

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

   since a is a quadratic residue and $p \equiv 1 \mod 4$.

4. (a) Calculate $\phi(7!)$.
   SOLUTION: Note that

$$7! = 1 \cdot 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot 2 \cdot 3 \cdot 7 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$$

   Hence

$$\phi(7!) = \phi(2^4)\phi(3^2)\phi(5)\phi(7) = 2^3 3 \cdot 2 \cdot 4 \cdot 6 = 2^7 3^2$$

   (b) Suppose p and q are twin primes, i.e. $q = p + 2$. Show that

$$\phi(q) = \phi(p) + 2$$

   SOLUTION: Since p and q are primes one has

$$\phi(q) = q - 1 = p + 2 - 1 = (p - 1) + 2 = \phi(p) + 2$$

   (c) Suppose

$$n = 2^{2^k}$$

   Find $\tau(n)$ and $\sigma(n)$.
   SOLUTION:

$$\tau(n) = 2^k + 1$$

$$\sigma(n) = 2^{2^k+1} - 1$$

5. Find the 8th convergent of $\sqrt{2}$

   As we saw in class, $\sqrt{2} = [1, \overline{2}]$. We find p_7/q_7 (if you found p_8/q_8, that's ok).

   $p_0 = 1, p_1 = 2+1 = 3, p_2 = 6+1 = 7, p_3 = 14+3 = 17, p_4 = 34+7 = 41, p_5 = 82+17 = 99, p_6 = 198 + 41 = 239, p_7 = 478 + 99 = 577$.

   $q_0 = 1, q_1 = 2 = 2, q_2 = 4 + 1 = 5, q_3 = 10 + 2 = 12, q_4 = 24 + 5 = 29, q_5 = 58 + 12 = 70, q_6 = 140 + 29 = 169, q_7 = 338 + 70 = 408$.

   Hence the eighth convergent, C_7 is $577/408$.

6. Suppose p is prime and $n \geq 2$ and $a^{p^2} \equiv 1 \mod n$. Show that $\text{ord}_n a = p^2$ if and only if $a^p \not\equiv 1 \mod n$.

   SOLUTION: Since $a^{p^2} \equiv 1 \mod n$ it follows that the order of a divides p^2. It is hence one of $1, p, p^2$ since p is a prime. It is then clear that the order is p^2 precisely when $a^p \not\equiv 1 \mod n$.

7. 9 is a square, so it is a quadratic residue modulo any prime that is relatively prime to 9. Hence it is a quadratic residue modulo all primes not equal to 3.

8. Find a number λ between 200 and 250 such that for every $n|\phi(\lambda)$ there exists an integer A such that $\text{ord}_\lambda(A) = n$.

   SOLUTION: 233 is a prime number, so there is a primitive root r mod 233. So, if $n|\phi(233) = 232$, we have that the order of $r^{232/n}$ is precisely n mod 233, since it is $\text{ord}_{233}(r)/(\text{ord}_{233}(r), 232/n) = 232/(232/n) = n$.

9. (a) State the Mobius inversion formula.

   (b) Show that for all $n \geq 1$ one has

$$\sum_{d|n} \tau(d)\mu(n/d) = 1$$

SOLUTION: Let

$$f = \tau * \mu$$

By Mobius inversion one has

$$\tau = f * \mathbf{1}$$

But one also has

$$\tau = \mathbf{1} * \mathbf{1}$$

Hence

$$(f * \mathbf{1}) * \mu = (\mathbf{1} * \mathbf{1}) * \mu$$

and hence

$$f * \delta = \mathbf{1} * \delta$$

and hence

$$f = \mathbf{1}$$

and this implies the desired result.

10. (a) Find all primitive roots modulo 23.

    First, note that 5 is a primitive root mod 23, since its order mod 23 must divide $\phi(23) = 22$, and so it must be $2, 11$, or 22. We have $5^2 \equiv 2$ and $5^1 1 = (5^2)^5 \cdot 5 \equiv 32 \cdot 5 \equiv 45 \not\equiv 1 \pmod{23}$, and so $\text{ord}_{23}(5) = 22$. Then we have that the set of primitive roots is $5, 5^3, 5^5, 5^7, 5^9, 5^{13}, 5^{15}, 5^{17}, 5^{19}, 5^{21}$, since all of these powers have gcd 1 with $\text{ord}_{23}(5) = 22$.

    (b) How many primitive roots are there modulo 171?

    SOLUTION: 171 is $9 \cdot 19$, and by the primitive root theorem there are no primitive roots modulo a number of this form (since it is not a power of a prime, or twice the power of a prime).

    (c) How many primitive roots are there modulo 173?

    SOLUTION: 173 is prime, so there are $\phi(\phi(173)) = \phi(172) = \phi(4 \cdot 43) = 2 \cdot 42 = 84$ primitive roots $\pmod 1$73.

11. How many primitive roots are there modulo 26^{100}?

    SOLUTION: None: by the Primitive Root Theorem, only modulo numbers of the form 1, 2, 4, p^m, and $2 \cdot p^m$ where p is an odd prime and $m \geq 1$ is an integer can one have a primitive root.

12. Find the order of 12 modulo 35.

    SOLUTION: We have that this order must divide $\phi(35) = 24$, and cannot be 24 since there are no primitive roots modulo 35. Hence we check that

    $$12^2 \equiv 4 \pmod{35},\ 12^3 \equiv 13 \pmod{35},\ 12^4 \equiv 16 \pmod{35},\ 12^6 \equiv 29 \pmod{35}.$$

    The only remaining possible order is 12 is 12, so this is the order.

    $$\text{ord}_{35}(12) = 12$$

13. Write down the continued fraction expansion for $\sqrt{29}$. Find its first five convergents.

    SOLUTION: $\lfloor \sqrt{29} \rfloor = 5$, so the first term of the expansion is 5. The next term is

    $$\left\lfloor \frac{1}{\sqrt{29} - 5} \right\rfloor = \left\lfloor \frac{\sqrt{29} + 5}{4} \right\rfloor = 2.$$

    The next term is

    $$\left\lfloor 1/(\frac{\sqrt{29} + 5}{4} - 2) \right\rfloor = \left\lfloor \frac{4}{\sqrt{29} - 3} \right\rfloor = \left\lfloor \frac{4\sqrt{29} + 12}{20} \right\rfloor = \left\lfloor \frac{\sqrt{29} + 3}{5} \right\rfloor = 1.$$

The next term is

$$\left\lfloor 1/(\frac{\sqrt{29}+3}{5}-1)\right\rfloor = \left\lfloor \frac{5}{\sqrt{29}-2}\right\rfloor = \left\lfloor \frac{5\sqrt{29}+10}{25}\right\rfloor = \left\lfloor \frac{\sqrt{29}+2}{5}\right\rfloor = 1.$$

The next term is

$$\left\lfloor 1/(\frac{\sqrt{29}+2}{5}-1)\right\rfloor = \left\lfloor \frac{5}{\sqrt{29}-3}\right\rfloor = \left\lfloor \frac{5\sqrt{29}+15}{20}\right\rfloor = \left\lfloor \frac{\sqrt{29}+3}{4}\right\rfloor = 2.$$

The next term is

$$\left\lfloor 1/(\frac{\sqrt{29}+3}{4}-2)\right\rfloor = \left\lfloor \frac{4}{\sqrt{29}-5}\right\rfloor = \left\lfloor \frac{4\sqrt{29}+20}{4}\right\rfloor = \left\lfloor \sqrt{29}+5\right\rfloor = 10.$$

The next term is

$$\left\lfloor \frac{1}{\sqrt{29}-5}\right\rfloor = 2$$

from before. Clearly, from now on the terms will repeat the period $2, 1, 1, 2, 10$, so the continued fraction expansion is

$$\sqrt{29} = [5, \overline{2, 1, 1, 2, 10}].$$

The first five convergents are

$$5, [5, 2], [5, 2, 1], [5, 2, 1, 1], [5, 2, 1, 1, 2],$$

which are $5, 11/2, 16/3, 27/5, 70/13$.

14. Which quadratic irrational does the continued fraction $[4, \overline{2, 1}]$ correspond to?

SOLUTION: First we note that if $\beta = [\overline{2, 1}]$, then

$$\beta = 2 + \frac{1}{1+\frac{1}{\beta}},$$

so

$$1 = \frac{2}{\beta} + \frac{1}{\beta+1}$$

, so

$$\beta^2 + \beta = 2\beta + 2 + \beta = 3\beta + 2$$

, and so $\beta^2 - 2\beta - 2 = 0$, meaning

$$\beta = \frac{2+\sqrt{4+8}}{2} \text{ or } \beta = \frac{2-\sqrt{4+8}}{2}$$

It cannot be the latter, as it is positive, so $\beta = 1 + \sqrt{3}$. Now, we have

$$[4, \overline{2, 1}] = 4 + \frac{1}{\beta} = 4 + \frac{1}{1 + \sqrt{3}} = 4 + \frac{\sqrt{3} - 1}{2} = \frac{\sqrt{3} + 7}{2}.$$

15. For which positive integers a is $(a + \sqrt{5})/3$ expressed as an eventually periodic continued fraction? A periodic continued fraction?

    SOLUTION: Since this is a quadratic irrational for all integers a, it has an eventually periodic continued fraction for all integers a. This will have a periodic continued fraction for $a = 1$ or 2. See the last page for the justification.

16. Find two continued fraction expansions for $\frac{13}{5}$. Are there others? Why or why not?

    SOLUTION: Run the Euclidean algorithm on $(13, 5)$ and get

$$13 = 2 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1.$$

Thus one continued fraction expansion of $13/5$ is $[2, 1, 1, 2]$, and another is $[2, 1, 1, 1, 1]$, since $1/2 = 1/(1 + 1/1)$. These are the only two expansions, since rational numbers always have exactly two expansions, as proven on the homework.

17. Show that $\frac{5042}{2911}$ is a convergent of $\sqrt{3} = 1.7320508075\ldots$.

    This isn't a great practice problem, because its best done with a calculator. However, it helps us to recall an important result. If you compute $|\sqrt{3} - \frac{5042}{2911}|$, this is

$$0.000000034066 \cdots < \frac{1}{2(2911)^2} = 0.000000059005,$$

and so this must be a convergent by a theorem shown in class.

18. Which of the following can be written as a sum of two squares? A sum of three squares? Four squares?

    (a) 39470

    (b) 55555

    (c) 34578

(d) 12!

(e) A number of the form $p^2 + 2$, where p is a prime.

SOLUTION: For the first three of these, one first writes down the prime factorizations: they are $2 \cdot 5 \cdot 3947$, $5 \cdot 41 \cdot 271$, $2 \cdot 3^2 \cdot 17 \cdot 113$. All of these contain primes in the prime factorization which are 3 mod 4 but not taken to an even power, so none are sums of two squares. Also, 3 is a prime divisor of 12!, but it divides 12! exactly up to the fifth power, which is not even, and hence 12! is also not a sum of two squares. Finally, for the last example, if p is even, $p^2 + 2 = 6$ which is not a sum of two squares, and $p^2 + 2 \equiv 3 \pmod 4$ if p is odd, so this is never a sum of two squares.

Now we check for sums of three squares. The only numbers not expressible as sums of three squares are of the form $4^m(8n + 7)$. None of the first three examples are divisible by a power of 4, so we just check them mod 8. The first example is even mod 8, the second example is 3 mod 8, so it can be written as a sum of three squares. The third example is again even mod 8, and so it also can be written as a sum of three squares. The fourth example is $4^5 \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11$, where $3^5 \cdot 5^2 \cdot 7 \cdot 11$ is 7 mod 8, so it cannot be written as a sum of three squares. The last example can always be written as $p^2+1^2+1^2$.

All of these can be written as a sum of four squares, since all integers can be.

19. Suppose $x \in \mathbb{Z}^{>0}$ can be written as a sum of two squares. What is the necessary and sufficient condition on $y \in \mathbb{Z}^{>0}$ for xy to be expressible as a sum of two squares?

    SOLUTION: The necessary and sufficient condition is that y is a sum of two squares. It is sufficient because the product of two integers that are sums of two squares is also a sum of two squares. To see that it is necessary, suppose y cannot be written as a sum of two squares, but x can. FIrst of all, this means that there is a prime that is 3 mod 4 and such that the highest power of p dividing y is an odd power. Second of all, whenever p is such a prime, the highest power of p dividing x is even (maybe 0). So the highest power of p dividing xy is odd, and so xy cannot be written as a sum of two squares.

20. Show that the area of any right triangle with all integer sides is divisible by 6.

    SOLUTION: Given the parametrization of primitive Pythagorean triples (x, y, z), we have that

$$x = m^2 - n^2, y = 2mn, z = m^+n^2$$

for some integers m, n which are relatively prime, and such that exactly one of them is even. Since one of them is even, y is divisible by 4. Suppose m is even, n is odd, and neither is divisible by 3. Then both m^2 and n^2 have to be 1 mod 3, and so x is divisible by 3, and the area, $xy/2$, is divisible by $12/2 = 6$. If one of m, n is divisible by 3, then y is divisible by 12 and so the area is divisible by 6.

21. Which primes p can be the hypotenuse (i.e. largest integer) in a primitive Pythagorean triple? Justify your answer.

SOLUTION: In a primitive Pythagorean triple, the hypotenuse is always a sum of two squares, $m^2 + n^2$. Hence any prime that is $1 \pmod 4$ can be the hypotenuse of a PPT, and no others (2 is not a hypotenuse for a PPT). Note that if the hypotenuse is prime, then the triple must be primitive unless one of the legs is 0. This would mean either m or n is 0 (not possible since p is not a square) or that $m = n$, which would mean $p = 2m^2$ which is true for no prime except 2.

(15) We consider 3 cases.

- $a = 3k$ for some $k \in \mathbb{Z}$

$$\Rightarrow \frac{a+\sqrt{5}}{3} = k + \frac{\sqrt{5}}{3} = k + [0, 1, \overline{2, 1, 12, 1, 2, 2}]$$
$$= [k, 1, \overline{2, 1, 12, 1, 2, 2}]$$

(we leave the computation of the c.f. of $\sqrt{5}/3$ to you)

No matter what k is (you can try $k = 1, 2,$ or 12 to have a chance at making this (purely) periodic), this will not be periodic

- $a = 3k + 1$ for some $k \in \mathbb{Z}$

verify yourself

$$\Rightarrow \frac{a+\sqrt{5}}{3} = k + \frac{1+\sqrt{5}}{3} = k + [1, \overline{12, 1, 2, 2, 2, 1}]$$
$$= [k+1, \overline{12, 1, 2, 2, 2, 1}]$$

if $k = 0$, this is $[1, \overline{12, 1, 2, 2, 2, 1}] = [\overline{1, 12, 1, 2, 2, 2}$

no other value of k will make this periodic.

$k = 0 \Rightarrow \boxed{a = 1}$

- $a = 3k + 2$ for some $k \in \mathbb{Z}$.

$$\Rightarrow \frac{a+\sqrt{5}}{3} = k + \frac{2+\sqrt{5}}{3} = k + (1, \overline{2, 2, 2, 1, 12, 1}) = [k+1, \overline{2, 2, 2, 1, 1}$$

if $k = 0$, $[k+1, \overline{2, 2, 2, 1, 12, 1}] = [1, \overline{2, 2, 2, 1, 12, 1}] = [\overline{1, 2, 2, 2, 1, 12}$

no other value of k makes this periodic.

$k = 0 \Rightarrow \boxed{a = 2}$.

NOTE: This is a good problem for practicing for the exam. If you can do this you have infinite c.f.'s down.