# Practice Final

*Note: This practice final has a bias towards things not covered on the midterm, since you have fewer materials from that section of the course to help you study. However, on the final all topics should be represented equally.*

1. True or false:
   (a) If $a$ is a sum of three squares, and $b$ is a sum of three squares, then so is $ab$.
   (b) No number of the form $4^m(8n+7)$ can 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 $p$.
   (d) A perfect number must have at least four divisors.
   (e) An infinite simple continued fraction never converges to a rational number.

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

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

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 $p$.

4. (a) Calculate $\phi(7!)$.
   (b) Suppose $p$ and $q$ are twin primes, i.e. $q = p + 2$. Show that

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

   (c) Suppose

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

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

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

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 $a^p \not\equiv 1 \mod n$.

7. Describe all primes modulo which 9 is a quadratic residue.

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

9. (a) State the Mobius inversion formula.

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

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

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

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

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

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

12. Find the order of 12 modulo 35.

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

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

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

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

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

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.

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?

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

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