Solutions to Final Examination, 8:00–10:00 am, May 14, 2025

Instructions: Attempt all questions. Closed book; however, a ‘cheat sheet’ (one 8.5″×11″ sheet with your own handwriting) and a calculator are permitted. *Answer clearly and precisely.* Total value of questions: 100 points (plus 20 bonus points available).

---

1. Find a solution of $x^2+y^2=z^4$ in positive integers x,y,z.

One small solution is $(15,20,5)$ is found by scaling $3^2+4^2=5^2$ by 25, and rewriting as $15^2+20^2=25^2=5^4$. In the same way, *every* Pythagorean triple (a,b,c) gives rise to a solution (ac,bc,c) of our equation. Of course none of these solutions have x,y,z relatively prime, and that is fine.

If you prefer primitive solutions, these are also not hard to find; for example, $7^2+24^2=5^4$. This arises from the observation that we are asking for a primitive Pythagorean triple $(m^2-n^2, 2mn, m^2+n^2)$ in which m^2+n^2 is itself a square. The case $(m,n)=(4,3)$ leads to $7^2+24^2=5^4$; and infinitely many more primitive solutions are found in this way.

2. Show that the equation $x^2-y^2=270$ has no integer solution.

For any integers x,y, we have $x^2-y^2\equiv 0,1,$ or $3 \mod 4$. Since $270\equiv 2 \mod 4$, there is no integer solution.

3. Compute each of the following.

   (a) $\phi(103)=102$ since 103 is prime.

   (b) the inverse of 31 mod 103 is 10. By the extended Euclidean algorithm, we have $\gcd(31,103)=1=10{\cdot}31-3{\cdot}103=1$.

   (c) Legendre symbol $\left(\frac{65}{103}\right)=\left(\frac{5}{103}\right)\left(\frac{13}{103}\right)=\left(\frac{103}{5}\right)\left(\frac{103}{13}\right)=\left(\frac{3}{5}\right)\left(\frac{-1}{13}\right)=(-1)(1)=-1.$

   (d) $\left(\frac{1}{103}\right)+\left(\frac{2}{103}\right)+\cdots+\left(\frac{102}{103}\right)=0$ since there are 51 squares and 51 nonsquares in $\mathbb{F}_{103}$.

4. Find the smallest positive integer x satisfying

$$x\equiv 19 \mod 61 \qquad\text{and}\qquad x\equiv 22 \mod 71.$$

Show your work.

For some k, $x=61k+19\equiv 22 \mod 71$, and $61k\equiv 3 \mod 71$. By the extended Euclidean algorithm, $\gcd(61,71)=1=7{\cdot}61-6{\cdot}71$; so the inverse of 61 mod 71 is 7. In our congruence for k, multiply both sides by 7 to obtain $k\equiv 21 \mod 71$; thus $k=71r+21$

and $x = 61(71k{+}21) + 19 = 4331r{+}1300$ for some integer r. All solutions satisfy $x \equiv 1300 \mod 4331$; and the smallest solution is $x = 1300$.

5. Find the exact value of the real number represented by the repeating continued fraction $\beta = [4, 1, 4, 1, 4, 1, 4, 1, 4, \ldots]$. Simplify your answer.

From $\beta = 4 + \frac{1}{1+\frac{1}{\beta}} = 4 + \frac{\beta}{1+\beta}$, we obtain $(\beta - 4)(1 + \beta) = \beta$, so $\beta^2 - 4\beta - 4 = 0$ and $\beta = \frac{1}{2}\big(4 \pm \sqrt{32}\big) = 2 \pm \sqrt{8}$. Since $\beta > 4$, we must have $\beta = 2 + \sqrt{8}$.

6. Find an integer solution of Pell's equation $x^2 - 6y^2 = 1$ with $x > 100$.

The smallest integer solution is $(x, y) = (5, 2)$, as found by inspection. (If this had been a larger problem, you would have used the continued fraction method to find this.) Other solutions are found as powers of $\alpha = 5{+}2\sqrt{6}$. For $n = 0, 1, 2, \ldots$ we have

$$\alpha^n = 1,\ 5{+}2\sqrt{6},\ 49{+}20\sqrt{6},\ 485{+}198\sqrt{6},\ 4801{+}1960\sqrt{6},\ 47525{+}19402\sqrt{6},\ \ldots.$$

So the smallest solution with $x > 100$ is $(x, y) = (485, 198)$.

7. We are given an integer $p > 1$. Suppose that $a^{p-1} \equiv 1 \mod p$ for every integer $a \in \{1, 2, 3, \ldots, p{-}1\}$. Does it necessarily follow that p is prime? Explain.

Yes, from the information given, we do know that p is prime. If p were composite, then p would have a divisor $a \in \{2, 3, \ldots, p{-}1\}$ satisfying $\gcd(a, p) = a$. This is not possible since $a^{p-1} \equiv 1 \mod p$ which forces $\gcd(a, p) = 1$.

Of course, it is impractical to use this procedure for testing primality; it is a valid algorithm but it takes exponential time. Rather than testing $a^{p-1} \equiv 1 \mod p$ for every a, it would be faster to test directly that a does not divide p. But this would be simply 'trial division', which is the most naive algorithm for testing primality; and it is extremely inefficient.

8. Answer TRUE or FALSE to each of the following statements.

(a) The sum of reciprocals of the primes is $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \cdots = \frac{\pi^2}{6}$.
False. Euler showed that the sum of the reciprocals of the primes diverges. By the way, the value $\frac{\pi^2}{6}$ is the sum of a very different series for $\zeta(2)$.

(b) There are infinitely many natural numbers n for which $4^n - 1$ is prime.
False. $4^n{-}1 = (2^n{+}1)(2^n{-}1)$ is not prime unless $n = 1$.

(c) There are infinitely many primes expressible as a sum of two integer squares.
True. By Dirichlet's Theorem, there are infinitely many primes $p \equiv 1 \mod 4$; and as explained in class, every such prime is expressible (efficiently, and in an essentially unique way) as a sum of two squares.

(d) There are infinitely many primes having '69' as the last two decimal digits (i.e. infinitely many primes p satisfying $p \equiv 69 \mod 100$).

True. By Dirichlet's Theorem, the arithmetic progression 69, 169, 269, 369, ... contains infinitely many primes.

(e) If m is an odd positive integer, then Euler's function satisfies $\phi(4m) = 2\phi(m)$.
True. Since $\gcd(m,4) = 1$, we have $\phi(4m) = \phi(4)\phi(m) = 2\phi(m)$.

(f) There are infinitely many primes p such that $3^p \equiv 5 \mod p$.
False. The only prime satisfying the indicated congruence is $p = 2$. If $p > 3$, then by Fermat's Little Theorem, $3^p \equiv 3 \not\equiv 5 \mod p$.

(g) If d, m are relatively prime positive integers, then the equation $x^2 - dy^2 = m$ must have positive integer solutions.
False. The equation $x^2 - 3y^2 = 7$ has no integer solutions, since the left side is congruent to 0, 1 or 2 mod 4. Similarly, $x^2 - 5y^2 = 2$ has no integer solutions, since the left side is congruent to 0, 1 or 3 mod 4. Also, $x^2 - 3y^2 = 2$ has no integer solutions since the left side is congruent to 0 or 1 mod 3.

(h) If the Legendre symbol $\left(\frac{a}{p}\right) = 1$ where a and p are large integers with p prime, then there is efficient algorithm to solve $x^2 \equiv a \mod p$. (Assuming a, p are less than 1000 decimal digits in length, an 'efficient' algorithm should find solutions in less than a minute on my laptop.)
True. In class, we demonstrated finding square roots mod p; and we stressed that this is a practical and efficient algorithm, with only a small caveat: It requires first finding a nonsquare mod p, and the algorithm for this is randomized (just like flipping a coin until we get heads). In human experience, the algorithm has always required less than one second. Currently, the only assurance that the algorithm runs in deterministic polynomial time, is a conditional result relying on a generalization of the Riemann Hypothesis. Now as mathematicians, we are deeply interested in questions about the Riemann Hypothesis. But this caveat raises only a theoretical question which is universally considered to be of no practical concern. True, there is *no absolute guarantee* that an example could never take more than a minute; but even if the Riemann Hypothesis is false, the chance of an example taking more than a minute is extremely remote, less than the chance of all life on earth being obliterated by a giant solar flare in the middle of the computation.

(i) Recent progress in generating large Mersenne primes, the largest of which have several millions of digits, has practical applications in modern implementations of RSA public key encryption where the choice of parameter $n = pq$ requires such large primes p and q for security reasons.
False. The primes that are useful in practical cryptography are generally secret, and have at most a few hundred digits. Mersenne primes are publicly known, and the largest ones (which is where all the recent progress lies) are millions of digits long, and these have no role in cryptographic applications.

(j) A solution of the Riemann Hypothesis would allow large integers to be factored in polynomial time.

False. As explained in class, the Riemann Hypothesis is of more theoretical interest. See our answer to (i) for an example of the relevance of the Riemann Hypothesis in computation. Whether the Riemann Hypothesis is ultimately proved, or remains forever a conjecture, does not change the way the best algorithms are designed and implemented.