Math 406, Test III, Spring 2015

Dr. Holmes

April 25, 2021

There are four computational questions and four proof questions. You may drop one of each. In addition, there is a bonus proof question which you may write if you are prepared for it.

1. Construct a number in mod 28907 arithmetic which has more than two square roots, list the square roots and provide calculations confirming that the two smallest square roots are indeed square roots of the same number. It might be useful to note that $28907 = (137)(211)$.

   (since this question is literally on the Spring 2021 second exam, I will of course not answer it. But you can see that I have asked such a question before).

2. Determine using Korselt's Criterion whether the following numbers are Carmichael numbers. Their prime factorizations are given. Show supporting calculations.

   $1105 = 5 \cdot 13 \cdot 17$

   $1235 = 5 \cdot 13 \cdot 19$

   $2820 = 7 \cdot 13 \cdot 31$

   $19747 = 7^2 \cdot 13 \cdot 31$

3. Find a Rabin-Miller misleader for mod 25 arithmetic (there is one, and it occurs fairly early if you consider residues in the natural order; this is not to say you don't have to compute for a bit). If you look below, you will find the statement of the Rabin-Miller theorem, from which you can back figure what the definition of a Rabin-Miller misleader must be. To get you started, note that $25 - 1 = 2^3 \cdot 3$. You may use Fermat's Little Theorem in your argument without proof.

4. I attach section 25 of the notes. Compute two square triangular numbers larger than 36. Verify that they are in fact square triangular numbers.

5. Prove that if p is a prime and $x \equiv y \bmod p$, then $x^p \equiv y^p \bmod p^2$. Make sure you make all the needed remarks to support the (not terribly long) proof.

6. Prove that there are infinitely many primes of the form $4n + 3$ (this is the easier result which does **not** require any use of quadratic reciprocity, just facts about modular arithmetic).

7. Prove that each positive integer can be factored into primes in one and only one way (up to order of factors). There are two parts: first prove that each positive integer is a prime or a product of a finite number of primes (so there is at least one prime factorization); then prove that (up to order of factors) there is only one such factorization. The method of least counterexample is helpful in both cases. You may use Euclid's Lemma, that if p is a prime and $p|ab$, it follows that $p|a$ or $p|b$, and you may further extend this to finite products ($p|a_1 \cdot a_2 \cdot \ldots a_n \rightarrow p|a_i$ for some i).

8. (success on this question may improve your grade on Test II as well) Prove the Rabin-Miller theorem: if p is an odd prime and $p-1 = 2^k q$, q odd, and $1 < a < p$, then either $a^q \equiv_p 1$ or for some $i \in [0, k-1]$, $a^{2^i q} \equiv -1$.

9. **bonus proof question** Prove that 2 is a quadratic residue mod p (for p an odd prime) iff $p \equiv_8 1$ or $p \equiv_8 7$. You may assume Euler's Criterion as already established in your proof.