MATH 467 FACTORIZATION AND PRIMALITY TESTING, FALL 2023, PROBLEMS 6

Return by Monday 9th October

This week's questions require some computational aids, such as Pari or Mathematica. When you write a computer program to solve the problem your code must be submitted along with your solutions.

1. Given that n is a product of two primes p and q with $p \le q$, prove that

$$p = \frac{n+1-\phi(n)-\sqrt{(n+1-\phi(n))^2-4n}}{2}.$$

When $n = 19749361535894833$ and $\phi(n) = 19749361232517120$ use this to find p and q.

2. A "probable prime" p is a number such that $a^{p-1} \equiv 1 \pmod{p}$ for $a = 2, 3, 5, 7$. For each of the odd numbers n with $100000000000 \le n \le 100000000025$ list the ones which are probable primes and for those which are not list the values of a for which the test fails.

3. Find all n such that $\phi(n) = 12$.

4. Show that 3 is a primitive root modulo 17 and draw up a table of discrete logarithms to this base modulo 17. Hence, or otherwise, find all solutions to the following congruences.
   (i) $x^{12} \equiv 16 \pmod{17}$,
   (ii) $x^{48} \equiv 9 \pmod{17}$,
   (iii) $x^{20} \equiv 13 \pmod{17}$,
   (iv) $x^{11} \equiv 9 \pmod{17}$.

5. Suppose that p is an odd prime and g is a primitive root modulo p. Prove that g is a quadratic non-residue modulo p.