MATH 467 FACTORIZATION AND PRIMALITY TESTING, FALL 2024, PROBLEMS 6

Return by Monday 7th October

1. Find all solutions (if there are any) to each of the following congruences
(i) $x^2 \equiv -1 \pmod 7$, (ii) $x^2 \equiv -1 \pmod{13}$, (iii) $x^5 + 4x \equiv 0 \pmod 5$.

2. Given that n is a product of two primes p and q with $p < q$, 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.

3. Suppose that you have set up a public key and someone has sent you a secret message s

$$3136221279868451438935411629353487979528543803675 96$$

Given that your modulus n is

$$24479520371121008474792131183260228434377050031262 89$$

and your secret key d is

$$13804591050729758078634865863849864388970507684210 05$$

decode the message. You may assume that the message is encoded using the ASCII codes of letters and symbols https : //www.asciitable.com/

4. First find a primitive root modulo 19 and then find all primitive roots modulo 19.

5. 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) $x^{11} \equiv 9 \pmod{17}$.