Math 467 Factorization and Primality Testing, Fall 2024, Solutions 6

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) $x^5 + 4x \equiv 0 \pmod{5}$.

(i) No solutions. (ii) $x \equiv 5$ and $8 \pmod{13}$. (iii) $x \equiv 0, 1, 2, 3, 4 \pmod{5}$.

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.

We have $n = pq$, $\phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - p - q + 1$, $p + q = n + 1 - \phi(n)$. Thus p, q are the roots of $x^2 - (n + 1 - \phi(n))x + n = 0$. They are 94591153, 208786561.

3. Decode a secret message s, with modulus n and your secret key d where

$$\begin{aligned} s &= 31362212798684514389354116293534879795285438036759 6\\ n &= 2447952037112100847479213118326022843437705003126289\\ d &= 1380459105072975807863486586384986438897050768421005\\ m &= 067111110103114097116117108097116105111110115033033 \end{aligned}$$

Congratulations!

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

Checking $2^k \pmod{19}$ for $k = 2, 3, 6, 9$, the proper divisors of $\phi(19) = 18$ shows that 2 is a primitive root modulo 19. Then the numbers 2^m with $1 \le m \le 18$ and $(m, 18) = 1$ give all the primitive roots. $m = 1, 5, 7, 11, 13, 17$. Thus the primitive roots are 2, $3 \equiv 2^{13} \pmod{19}$, $10 \equiv 2^{17} \pmod{19}, 13 \equiv 2^5 \pmod{19}$, $14 \equiv 2^7 \pmod{19}$, $15 \equiv 2^{11} \pmod{19}$.

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

y	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^y	1	3	9	10	13	5	15	11	6	14	8	7	4	12	2	6
x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{dlog}_3 x$	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

(i) $12y \equiv 8 \pmod{16}$, $3y \equiv 2 \pmod{4}$, $y \equiv 2 \pmod{4}$, $y \equiv 2$, 6, 10 or 14 $\pmod{16}$. $x \equiv 9$, 15, 8 or 2 $\pmod{17}$. (ii) $48y \equiv 2 \pmod{16}$. $(48, 16) = 16 \nmid 2$ so no solutions. (iii) $20y \equiv 4 \pmod{16}$. $y \equiv 5y \equiv 1 \pmod{4}$ so $y \equiv 1$, 5, 9, 13 $\pmod{16}$ and $x \equiv 3$, 5, 14, 12 $\pmod{17}$. (iv) $11y \equiv 2 \pmod{16}$, $y \equiv 6 \pmod{16}$, $x \equiv 15 \pmod{17}$.