MATH 430 Problem Set 6

Qilin Ye

October 29, 2020

Problem 1

Use the Miller-Rabin test on the following two numbers. In each case, either provide a Miller-Rabin witness for the compositeness of N or conclude that N is probably prime by providing 3 numbers that are not Miller-Rabin witnesses for N.

(1) $N = 118901527$

(2) $N = 118901521$

Solution

(1) First factorize $N - 1 = 118901526 = 2 \cdot 59450763 =: 2k$. Here we only need to check if a^k is neither 1 nor $-1 \bmod N$.

$$\begin{aligned} 2^k &\equiv \ \ 1 \pmod N, \text{ fail} \\ 3^k &\equiv -1 \pmod N, \text{ fail} \\ 5^k &\equiv -1 \pmod N, \text{ fail} \end{aligned}$$

With the existence of three nonwitnesses, we conclude that N is likely to be prime.

(2) In this case, $N - 1 = 2^4 \cdot 7431345 =: 2^4 \cdot k$. We start by testing whether 2 is a witness.

$$\begin{aligned} 2^k &\equiv 45274074 \pmod N && \text{condition 1 met, proceed} \\ 2^{2k} &\equiv 1758249 \pmod N && \text{not failing condition 2, proceed} \\ 2^{4k} &\equiv 1 \pmod N && \text{not failing condition 2, proceed} \\ 2^{8k} &\equiv 1 \pmod N && \text{condition 2 met; witness found; } \texttt{return true} \end{aligned}$$

Indeed it is, and so N is composite.

Problem 2

Find *all* integers $0 \leqslant a \leqslant 76$ that are solutions to the equation $x^2 - 1 \equiv 0 \pmod{77}$. Can you generalize to finding all solutions to $x^2 - 1 \equiv 0 \pmod{pq}$ where p, q are distinct odd primes?

Solution

If $x^2 - 1 \equiv 0 \pmod{77}$ then $77 \mid x^2 - 1 = (x+1)(x-1)$. Since $77 = 7 \cdot 11$, we have four possible cases here:

(1) $77 \mid x - 1 \implies x \equiv 1 \pmod{77} \implies x = 1$.

(2) $77 \mid x + 1 \implies x \equiv 76 \pmod{77} \implies x = 76$.

(3) $7 \mid (x-1)$ and $11 \mid (x+1)$. In this case we need to solve the system of linear congruences

$$x \equiv 1 \pmod{7} \text{ and } x \equiv 10 \pmod{11}$$

which gives us $x \equiv 43 \pmod{77} \implies x = 43$.

(4) $7 \mid (x+1)$ and $11 \mid (x-1)$, in which case we need to solve

$$x \equiv 6 \pmod{7} \text{ and } x \equiv 1 \pmod{11}$$

from which we get $x \equiv 34 \pmod{77} \implies x = 34$.

The four solutions above are *all* possible solutions.

Remark

The same logic follows if we replace 77 by the product of two distinct odd primes. Again, four cases: the first two give us $x = 1$ and $x = pq - 1$. The other two requires us to solve the following two systems.

$$\begin{cases} x \equiv 1 \pmod{p} \\ x \equiv q - 1 \pmod{q} \end{cases} \quad \text{and} \quad \begin{cases} x \equiv 1 \pmod{q} \\ x \equiv p - 1 \pmod{p} \end{cases}$$

Problem 3

Use the data provided to find a nontrivial factor of $N = 198103$.

$$\begin{aligned}
1189^2 &\equiv 27000 \pmod{198103} \quad \text{and} \quad 27000 = 2^3 \cdot 3^3 \cdot 5^3 \\
1605^2 &\equiv 686 \pmod{198103} \quad \text{and} \quad 686 = 2 \cdot 7^3 \\
2378^2 &\equiv 108000 \pmod{198103} \quad \text{and} \quad 108000 = 2^5 \cdot 3^3 \cdot 5^3 \\
2815^2 &\equiv 105 \pmod{198103} \quad \text{and} \quad 105 = 3 \cdot 5 \cdot 7
\end{aligned}$$

Solution

I first tried to use the first and third line but it led to a trivial factorization. However, combining all but the third line works:

$$1189^2 \cdot 1605^2 \cdot 2815^2 \equiv 2^6 \cdot 3^6 \cdot 5^6 \cdot 7^6 \pmod{198103} \implies 198103 \mid (1189 \cdot 1605)^2 - 44100^2.$$

A "quick" verification suggests that

$$\gcd(1189 \cdot 1605 - 44100, 198103) = 499 \text{ and } \gcd(1189 \cdot 1605 + 44100, 198103) = 397.$$

From this we have obtained a factorization $198103 = 397 \cdot 499$.