M328K: Homework 8

Katherine Ho

November 4, 2024

1. Let $n > 1$ be odd and let $\gcd(a, n) = 1$. Show that if a is a quadratic residue of n, then the Jacobi symbol satisfies $\left(\dfrac{a}{n}\right) = 1$. Give a counterexample to show that the converse is false.

Proof. If a is a QR of n, then $x^2 \equiv a \pmod{n}$ has a solution. Then, $x^2 \equiv a \pmod{p_i}$ has a solution for every prime factor p_i of n. By definition of the Legendre symbol,

$$\left(\frac{a}{p_i}\right) = 1$$

for each prime factor p_i of n. Then the product of the Legendre symbols for each p_i is

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_k}\right) = 1$$

Thus if a is a quadratic residue of n, then the Jacobi symbol satisfies $\left(\dfrac{a}{n}\right) = 1$.

□

A counterexample is $a = 2$ and $n = 9$. The Jacobi symbol satisfies $\left(\frac{2}{9}\right) = 1$:

$$\left(\frac{2}{9}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{3}\right) = (-1)(-1) = 1$$

Now we check if 2 is a quadratic residue of 9 by calculating all of the QRs of 9.

$$\begin{aligned}
1^2 &\equiv 1 \pmod{9}\\
2^2 &\equiv 4 \pmod{9}\\
3^2 &\equiv 0 \pmod{9}\\
4^2 &\equiv 7 \pmod{9}\\
5^2 &\equiv 7 \pmod{9}\\
6^2 &\equiv 0 \pmod{9}\\
7^2 &\equiv 4 \pmod{9}\\
8^2 &\equiv 1 \pmod{9}
\end{aligned}$$

2 is not a quadratic residue of 9 and thus the converse is false.

2. Prove that there are infinitely many primes of the form $8k+7$. (Hint: Emulate the proof that there are infinitely many primes of the form $4k+1$, using $N = (4p_1 \cdots p_n)^2 - 2$.)

   Proof. Suppose that there are only a finite number of primes of the form $8k+7$. Let these primes be $p_1, \ldots, p_n$ s.t. $p_i \equiv 7 \pmod 8$. Consider $N = (4p_1 \ldots p_n)^2 - 2$. Let p be an odd prime dividing N. Note $p \neq p_i$ for any i, otherwise $p \mid (N - (4p_1 \ldots p_n)^2) = -2$. But since $p \mid ((4p_1 \ldots p_n)^2 - 2)$, we have

   $$(4p_1 \ldots p_n)^2 \equiv 2 \pmod p$$

   ie. $\left(\frac{2}{p}\right) = 1$, so $p \equiv 1, 7 \pmod 8$. So we have constructed another prime $\equiv 7 \pmod 8$ not in the original list. Thus there are infinitely many primes of the form $8k+7$.

   □

3. Let $n = 341$.

   (a) Apply the Fermat primality test to n using $a = 2$. What is the conclusion?

   Proof. Let $a = 2$.

   $$\text{If } 2^{340} \not\equiv 1 \pmod{341}, \text{ then 341 is composite.}$$

   The binary expansion of 2^{340} is

   $$2^{340} = 2^{256} \cdot 2^{64} \cdot 2^{16} \cdot 2^4$$

   Then find what each term is congruent to $\pmod{341}$.

   $$\begin{aligned} 2 &\equiv 2 \pmod{341} \\ 2^2 &\equiv 4 \\ 2^4 &\equiv 16 \\ 2^8 &\equiv 256 \\ 2^{16} &\equiv 256^2 \equiv 65536 \equiv 64 \\ 2^{32} &\equiv 64^2 \equiv 4096 \equiv 4 \\ 2^{64} &\equiv 4^2 \equiv 16 \\ 2^{128} &\equiv 16^2 \equiv 256 \\ 2^{256} &\equiv 256^2 \equiv 64 \end{aligned}$$

   By substitution,

   $$\begin{aligned} 2^{340} &\equiv 64 \cdot 16 \cdot 64 \cdot 16 \pmod{341} \\ &\equiv 4 \cdot 256 \pmod{341} \\ &\equiv 1 \pmod{341} \end{aligned}$$

   We have found that $2^{340} \equiv 1 \pmod{341}$, so the test is indeterminate.

   □

(b) Apply the Solovay–Strassen primality test to n using $a = 2$. What is the conclusion?

Proof. Let $a = 2$.

$$\text{If } 2^{\frac{341-1}{2}} \not\equiv \left(\frac{2}{341}\right) \pmod{341}, \text{ then 341 is composite.}$$

Evaluate $\left(\frac{2}{341}\right)$. Since $341 \equiv 5 \pmod 8$, $\left(\frac{2}{341}\right) = -1$.

Now by substitution, we can check

$$2^{170} \equiv -1 \pmod{341}$$

The binary expansion of 2^{170} is

$$2^{128} \cdot 2^{32} \cdot 2^{8} \cdot 2^{2}$$

By substitution,

$$\begin{aligned} 2^{170} &= 2^{128} \cdot 2^{32} \cdot 2^{8} \cdot 2^{2} \\ &\equiv 256 \cdot 4 \cdot 256 \cdot 2 \pmod{341} \\ &\equiv 64 \cdot 4 \cdot 2 \\ &\equiv 512 \pmod{341} \\ &\equiv 171 \pmod{341} \end{aligned}$$

$171 \not\equiv -1 \pmod{341}$, so we can conclude that 341 is composite.

$\square$