Quadratic reciprocity and its application in the Euler test


On the one hand, $8^{10} \mod 21 = 1$, but $\left( \frac{8}{21} \right) = \left( \frac{2}{21} \right) \left( \frac{2}{21} \right) = \left( \frac{2}{21} \right) = -1$ since 21≡5 mod 8.

2. Let’s try to determine if 1729 is prime or composite. This is an interesting number. Not only is it a Carmichael number, so $b^{1728} \equiv 1 \mod 1729$ for all $b$ relatively prime to 1729, but in fact $b^{864} \equiv 1 \mod 1729$ for all such $b$.

To show 1729 is composite, let’s pick $b = 305$. Then $305^{864} \equiv 1 \mod 1729$. Now let’s evaluate

$$\left( \frac{305}{1729} \right) = \frac{(-1)^{304} \cdot 1729}{305} \frac{1729}{305} \frac{204}{305} \frac{2}{305} \frac{51}{305} = \frac{51}{305} = \frac{(-1)^{50} \cdot 305}{51} = \frac{305}{51} = \frac{50}{51} \frac{25}{51} = \frac{(-1)^{25}}{51} = \frac{(-1) \cdot 24 \cdot 25}{4} \frac{51}{25} = \frac{(-1) \cdot 51}{25} = (-1) \cdot \left( \frac{1}{25} \right) = (-1) \cdot (+1) = (-1).$$

So 1729 is definitely composite.

How do we know that $\left( \frac{1}{n} \right) = 1$ without factoring $n$? (In some other example, the “25” might be some large number $n$.) Well, if we factor $n$ into its prime factors, then $\left( \frac{1}{p} \right) = 1$ for every prime $p$, since 1 is a square mod $p$. Hence $\left( \frac{1}{n} \right) = 1$ by the multiplicative property.

3. Let’s try to show 8911 is composite. Evaluate $\left( \frac{3001}{8911} \right)$:

$$\left( \frac{3001}{8911} \right) = (-1)^{8910 \cdot 3000} \left( \frac{8911}{3001} \right) = \left( \frac{8911}{3001} \right) = \left( \frac{2909}{3001} \right) = (-1)^{3000 \cdot 2908} \left( \frac{3001}{2909} \right) = \left( \frac{2909}{2909} \right) = \left( \frac{23}{23} \right) = \frac{11}{23}.$$

At this point it is not hard to check that 11 is NOT a square mod 23, but we can continue:

$$\left( \frac{11}{23} \right) = (-1)^{22 \cdot 10} \left( \frac{23}{11} \right) = -\left( \frac{23}{11} \right) = -\left( \frac{1}{11} \right) = -1.$$

Unfortunately, $3001^{4455} \equiv 1 \mod 8911$, so this doesn’t show 8911 is composite, but we know there is some $b$ which will show it is composite. If fact, let $b = 2$. Then $2^{8910} \equiv 1 \mod 8911$, so the Fermat
test doesn’t work, but \(2^{4455}\% 8911 = 6364\), so the Euler test tells us that 8911 is composite, even without evaluating a Jacobi symbol.