Math 322 Fall 2017
Number Theory Final Exam Practice Solutions

1. Let p be an odd prime. Show that -1 is a *quartic* (or fourth-power) residue if and only if $p \equiv 1 \mod 8$. (Hint: apply indices to the equation $x^4 \equiv -1 \mod p$).

   Solution: Let r be a primitive root, and consider the equation $x^4 \equiv -1 \mod p$. This is equivalent to $4 \operatorname{ind}_r x \equiv \operatorname{ind}_r(-1) \equiv (p-1)/2 \mod p-1$. If $p-1$ is divisible by 8 then this is equivalent to $\operatorname{ind}_r x \equiv (p-1)/8 \mod (p-1)/\gcd(p-1,4)$, which has a solution, and thus -1 is a quartic residue.

   Now for the converse assume $x^4 \equiv -1 \mod p$ has a solution, and set $y = \operatorname{ind}_r x$. We see that $-x$ is also a solution, and

   $$\operatorname{ind}_r(-x) \equiv \operatorname{ind}_r(-1) + \operatorname{ind}_r x \equiv (p-1)/2 + y \mod p-1.$$

   and thus we can assume without loss of generality that $0 \le y < (p-1)/2$.

   We have $4y \equiv (p-1)/2 \mod p-1$, and thus $4y = (p-1)/2 + k(p-1)$. But we know that $4y < 2(p-1)$ so either $4y = (p-1)/2$ or $4y = 3(p-1)/2$.

   In the first case, we have $8y + 1 = p$, and thus $p \equiv 1 \mod 8$. In the latter case we see that since $3 \not| 8$ we must have $3|y$, and get $8(y/3) + 1 = p$, and again $p \equiv 1 \mod 8$.

2. Evaluate $\left(\frac{7}{11}\right)$ and $\left(\frac{5}{13}\right)$ using Euler's criterion, and again using Gauss's lemma.

   Solution: By Euler's criterion, we have

   $$\left(\frac{7}{11}\right) \equiv 7^{(11-1)/2} \equiv 7^5 \equiv 5^2 \cdot 7 \equiv 3 \cdot 7 \equiv -1 \mod 11$$
   $$\left(\frac{5}{13}\right) \equiv 5^6 \equiv (-1)^3 \equiv -1 \mod 13.$$

   By Gauss's lemma, we see that

   $$7, 14, 21, 28, 35 \equiv 7, 3, 10, 6, 2$$

   has 3 elements greater than $11/2$, so $s = 3$ and $\left(\frac{7}{11}\right) = (-1)^3 = -1$.

   Similarly,
   $$5, 10, 15, 20, 25, 30 \equiv 5, 10, 2, 7, 12, 4$$
   has three elements greater than $13/2$ and thus $s = 3$, and we have $\left(\frac{5}{13}\right) = (-1)^3 = -1$.

3. Suppose a is a quadratic residue of an odd prime p. Show that $-a$ is a quadratic residue of p if and only if $p \equiv 1 \mod 4$.

Solution: We have

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

and we know that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \mod 4$. Thus $\left(\frac{-a}{p}\right) = 1$ if and only if $p \equiv 1 \mod 4$, and thus $-a$ is a quadratic residue if and only if $p \equiv 1 \mod 4$.

4. Evaluate $\left(\frac{3}{7}\right)$ and $\left(\frac{5}{11}\right)$ using Eisenstein's lemma.

Solution: We compute

$$\begin{aligned}
T(3,7) &= \lfloor 3/7 \rfloor + \lfloor 6/7 \rfloor + \lfloor 9/7 \rfloor = 0 + 0 + 1 = 1 \\
\left(\frac{3}{7}\right) &= (-1)^{T(3,7)} = (-1)^1 = -1 \\
T(5,11) &= \lfloor 5/11 \rfloor + \lfloor 10/11 \rfloor + \lfloor 15/11 \rfloor + \lfloor 20/11 \rfloor + \lfloor 25/11 \rfloor = 0 + 0 + 1 + 1 + 2 = 4 \\
\left(\frac{5}{11}\right) &= (-1)^{T(5,11)} = (-1)^4 = 1.
\end{aligned}$$

5. Calculate:

(a) $\left(\frac{3}{53}\right)$
(b) $\left(\frac{15}{101}\right)$
(c) $\left(\frac{31}{641}\right)$
(d) $\left(\frac{1009}{2307}\right)$ (This problem is poorly posed because the bottom is composite, sorry).
(e) $\left(\frac{2663}{3299}\right)$

Solution:

(a) $\left(\frac{3}{53}\right)\left(\frac{53}{3}\right) = 1$ so $\left(\frac{3}{53}\right) = \left(\frac{2}{3}\right) = -1$.

(b) $\left(\frac{15}{101}\right) = \left(\frac{3}{101}\right)\left(\frac{5}{101}\right)$.
$\left(\frac{3}{101}\right)\left(\frac{101}{3}\right) = (-1)^{2/2 \cdot 100/2} = 1$ so $\left(\frac{3}{101}\right) = \left(\frac{101}{3}\right) = \left(\frac{2}{3}\right) = -1$.
$\left(\frac{5}{101}\right)\left(\frac{101}{5}\right) = (-1)^{4/2 \cdot 100/2} = 1$ so $\left(\frac{5}{101}\right) = \left(\frac{101}{5}\right) = \left(\frac{1}{5}\right) = 1$.
Thus $\left(\frac{15}{101}\right) = (-1)(1) = -1$.

(c) $\left(\frac{31}{641}\right)\left(\frac{641}{31}\right) = 1$ so $\left(\frac{31}{641}\right) = \left(\frac{21}{31}\right)$.
$\left(\frac{21}{31}\right) = \left(\frac{3}{31}\right)\left(\frac{7}{31}\right)$.
$\left(\frac{3}{31}\right)\left(\frac{31}{3}\right) = (-1)^{2/2 \cdot 30/2} = (-1)$ so $\left(\frac{3}{31}\right) = -\left(\frac{31}{3}\right) = -\left(\frac{1}{3}\right) = -1$.
$\left(\frac{7}{31}\right)\left(\frac{31}{7}\right) = (-1)^{6/2 \cdot 30/2} = (-1)$ so $\left(\frac{7}{31}\right) = -\left(\frac{31}{7}\right) = -\left(\frac{3}{7}\right)$.
$\left(\frac{3}{7}\right)\left(\frac{7}{3}\right) = (-1)^{2/2 \cdot 6/2} = -1$ so $\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$.
Thus $\left(\frac{31}{641}\right) = (-1)(1) = -1$.

(d)

(e) $\left(\frac{2663}{3299}\right)\left(\frac{3299}{2663}\right) = -1$ so $\left(\frac{2663}{3299}\right) = -\left(\frac{3299}{2663}\right) = -\left(\frac{636}{2633}\right) = -\left(\frac{2^2}{2663}\right)\left(\frac{3}{2663}\right)\left(\frac{53}{2663}\right) = -\left(\frac{3}{2663}\right)\left(\frac{53}{2663}\right)$.
$\left(\frac{3}{2663}\right)\left(\frac{2663}{3}\right) = -1$ so $\left(\frac{3}{2663}\right) = -\left(\frac{2663}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$.
$\left(\frac{53}{2663}\right)\left(\frac{2663}{53}\right) = 1$ so $\left(\frac{53}{2663}\right) = \left(\frac{2663}{53}\right) = \left(\frac{13}{53}\right)$.
$\left(\frac{13}{53}\right)\left(\frac{53}{13}\right) = 1$ so $\left(\frac{13}{53}\right) = \left(\frac{53}{13}\right) = \left(\frac{1}{13}\right) = 1$.
Thus $\left(\frac{53}{2663}\right) = 1$, so $\left(\frac{2663}{3299}\right) = -\left(\frac{3}{2663}\right)\left(\frac{53}{2663}\right) = -(1)(1) = -1$.

6. Suppose p is an odd prime. Show that $\left(\frac{3}{p}\right)$ is 1 if $p \equiv \pm 1 \mod 12$ and is -1 if $p \equiv \pm 5 \mod 12$.

Solution: We have $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{2/2 \cdot (p-1)/2}$, which is 1 if $p \equiv 1 \mod 4$ and is -1 if $p \equiv -1 \mod 4$. Then we see that $\left(\frac{p}{3}\right) = 1$ if $p \equiv 1 \mod 3$ and is -1 if $p \equiv 2 \mod 3$. Using the Chinese Remainder Theorem to combine these facts, we get the desired conclusion.

7. Using the law of Quadratic Reciprocity, prove the following theorem:

Theorem 1. *Suppose p is an odd prime, $p \nmid a$, and q is a prime with $p \equiv \pm q \mod 4a$. Then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.*

This is in fact equivalent to the law of Quadratic Reciprocity, and is the form in which Euler originally proved it.

Solution: First assume a is odd. Then, using quadratic reciprocity, we have

$$\left(\frac{a}{p}\right)\left(\frac{p}{a}\right) = (-1)^{(p-1)/2(a-1)/2}$$
$$\left(\frac{a}{q}\right)\left(\frac{q}{a}\right) = (-1)^{(q-1)/2(a-1)/2}.$$

Since $q \equiv p \mod a$ we know that $\left(\frac{p}{a}\right) = \left(\frac{q}{a}\right)$, and since $p \equiv q \mod 4$ we know that $(p-1)/2 \equiv (q-1)/2 \mod 2$ and thus $(-1)^{(p-1)/2(a-1)/2} = (-1)^{(q-1)/2(a-1)/2}$. Thus $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Now suppose $a = 2^k b$ where b is odd. We have

$$\left(\frac{a}{p}\right) = \left(\frac{2^k}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{2^k}{p}\right)\left(\frac{b}{q}\right)$$
$$\left(\frac{2}{p}\right)(-1)^{(p^2-1)/8} = (-1)^{(q^2-1)/8}$$

since $p \equiv q \mod 4a$ and thus $p \equiv q \mod 8$. Thus $\left(\frac{a}{p}\right) = \left(\frac{2^k}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{2^k}{q}\right)\left(\frac{b}{q}\right) = \left(\frac{a}{q}\right)$.

8. Find a congruence describing all odd primes for which 5 is a quadratic residue.

Solution: Let p be an odd prime. Then $\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{2 \cdot (p-1)/2} = 1$ and thus $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. We can compute that p is a quadratic residue modulo 5 if $p \equiv 1 \mod 5$

or $p \equiv 4 \mod 5$, that is, if $p \equiv \pm 1 \mod 5$. Thus 5 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \mod 5$.

9. Let $p = 1 + 8 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 892,371,481$. This number is prime (don't bother trying to prove this yourself). Prove that if q is a prime and $q \leq 23$, then q is a quadratic residue modulo p.

   Conclude that there is no quadratic nonresidue of p less than 29, and thus no primitive root less than 29.

   Solution: Suppose $q \leq 23$ is an odd prime. Then we have

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)/2(q-1)/2} = 1$$

   since $8|p-1$. Thus

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = 1$$

   since $p \equiv 1 \mod q$. Thus q is a quadratic residue modulo p.

   Now we need to check 2 separately. We have see that $\left(\frac{2}{p}\right) = 1$ since $p \equiv 1 \mod 8$.

   Now suppose $1 \leq n \leq 28$. Then n is a product of primes ≤ 23, and since each of these primes is a quadratic residue modulo p, their product is also a quadratic residue modulo p (e.g. since the Legendre symbol is multiplicative). Thus n is a quadratic residue modulo p.

   Now suppose we have a primitive root r. We know that r must be a quadratic nonresidue modulo p, since $r^{(p-1)/2} \not\equiv 1 \mod p$ by definition of primitive root. Thus $r \not\leq 29$ by the previous argument.