Math 342 Tutorial

July 9, 2025

Question 1. Show that if $n = p_1^{2e_1+1} \cdots p_k^{2e_k+1} q_1^{2f_1} \cdots q_m^{2f_m}$, and if r is an odd prime not dividing n, then

$$\left(\frac{n}{r}\right) = \left(\frac{p_1}{r}\right) \cdots \left(\frac{p_k}{r}\right).$$

Using the fact that the Legendre symbol is totally multiplicative, we see at once that

$$\left(\frac{n}{r}\right) = \prod_{i=1}^{k} \underbrace{\left(\frac{p_1}{r}\right)^{2e_1}}_{=1} \left(\frac{p_1}{r}\right) \prod_{j=1}^{m} \underbrace{\left(\frac{q_1}{r}\right)^{2f_j}}_{=1} = \prod_{i=1}^{k} \left(\frac{p_1}{r}\right).$$

Question 2. Show that if p is odd prime that is 3 (mod 4), then $[(p-1)/2]! \equiv (-1)^t \pmod{p}$ where t is the number of nonquadratic residues in the range 0 to $\lfloor p/2 \rfloor$ inclusive.

In a similar manner as assignment 4 question 4, we see that $((p-1)/2)!^2 \equiv -(p-1)! \equiv 1 \pmod{p}$ by an application of Wilson's Theorem. By Euler's Criterion, we see that $((p-1)/2)!^{(p-1)/2} \equiv (1 \mid p)(2 \mid p) \cdots ((p-1)/2 \mid p) \equiv (-1)^t \pmod{p}$. Since $((p-1)/2)! \equiv \pm 1 \pmod{p}$, and since $(p-1)/2$ is odd, we're done.

Question 3. Let p be an odd prime. Prove the following identities. **(a)** $\sum_{r=1}^{p-1} r(r \mid p) = 0$ if $p \equiv 1 \pmod 4$. **(b)** $\sum_{\substack{r=1 \\ (r|p)=1}}^{p-1} r = \frac{p(p-1)}{4}$ if $p \equiv 1 \pmod 4$. **(c)** $\sum_{r=1}^{p-1} r^2(r \mid p) = p \sum_{r=1}^{p-1} r(r \mid p)$ if $p \equiv 3 \pmod p$. **(d)** $\sum_{r=1}^{p-1} r^3(r \mid p) = \frac{3}{2}p \sum_{r=1}^{p-1} r^2(r \mid p)$ if $p \equiv 1 \pmod 4$. **(e)** $\sum_{r=1}^{p-1} r^4(r \mid p) = 2p \sum_{r=1}^{p-1} r^3(r \mid p) - p^2 \sum_{r=1}^{p-1} r^2(r \mid p)$ if $p \equiv 3 \pmod 4$.

(a) Observe that $(r \mid p) = (-1)^{(p-1)/2}(p - r \mid r)$ (why?). Since $p \equiv 1 \pmod 4$, we then have

$$\sum_{r=1}^{p-1} r(r \mid p) = \sum_{r=1}^{p-1} (p-r)(p-r \mid p) = \sum_{r=1}^{p-1} (p-r)(r \mid p) = p \sum_{r=1}^{p-1} (r \mid p) - \sum_{r=1}^{p-1} r(r \mid p) = -\sum_{r=1}^{p-1} r(r \mid p).$$

(b) Since $p \equiv 1 \pmod 4$, we have

$$\sum_{\substack{r=1 \\ (r|p)=1}}^{p-1} r = \sum_{\substack{r=1 \\ (r|p)=1}}^{p-1} (p-r) = p \sum_{\substack{r=1 \\ (r|p)=1}}^{p-1} 1 - \sum_{\substack{r=1 \\ (r|p)=1}}^{p-1} r.$$

Solving for $\sum_{r=1,\,(r|p)=1}^{p-1} r$, and using the fact that there are $(p-1)/2$ quadratic residues modulo p, we obtain the result.

(c) Since $p \equiv 3 \pmod 4$, we have

$$\begin{aligned}
\sum_{r=1}^{p-1} r^2(r \mid p) &= \sum_{r=1}^{p-1} (p-r)^2(p-r \mid p) = -\sum_{r=1}^{p-1} (p-r)^2(r \mid p) \\
&= -p^2 \sum_{r=1}^{p-1} (r \mid p) + 2p \sum_{r=1}^{p-1} r(r \mid p) - \sum_{r=1}^{p-1} r^2(r \mid p) = 2p \sum_{r=1}^{p-1} r(r \mid p) - \sum_{r=1}^{p-1} r^2(r \mid p)
\end{aligned}$$

Solving for $\sum_{r=1}^{p-1} r^2(r \mid p)$ gives the result.

(d) For $p \equiv 1 \pmod 4$, we have that

$$\sum_{r=1}^{p-1} r^3(r \mid p) = \sum_{r=1}^{p-1}(p-r)^3(p-r \mid p) = \sum_{r=1}^{p-1}(p-r)^3(r \mid p)$$
$$= p^3\sum_{r=1}^{p-1}(r \mid p) - 3p^2\sum_{r=1}^{p-1} r(r \mid p) + 3p\sum_{r=1}^{p-1} r^2(r \mid p) - \sum_{r=1}^{p-1} r^3(r \mid p).$$

But $\sum_{r=1}^{p-1}(r \mid p) = 0$, and $\sum_{r=1}^{p-1} r(r \mid p) = 0$ by part (a). Hence, we obtain the result by solving for $\sum_{r=1}^{p-1} r^3(r \mid p)$.

(e) Since $p \equiv 3 \pmod 4$, we have

$$\sum_{r=1}^{p-1} r^4(r \mid p) = \sum_{r=1}^{p-1}(p-r)^4(p-r \mid p) = -\sum_{r=1}^{p-1}(p-r)^4(r \mid p)$$
$$= \sum_{i=0}^{4}(-1)^{i+1}\binom{4}{i}p^{4-j}\sum_{r=1}^{p-1} r^i(r \mid p).$$

From part (c), we know that $p\sum_{r=1}^{p-1} r(r \mid p) = \sum_{r=1}^{p-1} r^2(r \mid p)$. Substituting and solving, we obtain the result.

Question 4. Show that if a is a quadratic residue of the prime p, then the solutions of $x^2 \equiv a \pmod p$ are **(a)** $x \equiv \pm a^{n+1} \pmod p$ if $p = 4n+3$, or **(b)** $x \equiv \pm a^{n+1}$ or $\pm\, 2^{2n+1}a^{n+1} \pmod p$ if $p = 8n+5$.

(a) Since $p = 4n+3$, we have that

$$x^2 \equiv (\pm a^{n+1})^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2}a \equiv a \pmod 4.$$

Hence, the solutions in this case are $\pm a^{n+1} \pmod p$.

(b) Because $p \equiv 5 \pmod 8$, we know that -1 is a quadratic residue and 2 is a quadratic non-residues modulo p. Next, observe that $(\pm a^{n+1})^2 \equiv a^{(p+3)/4} \pmod p$ and $(\pm 2^{2n+1}a^{n+1}) \equiv 2^{(p-1)/2}a^{(p+3)/2} \equiv -a^{(p+3)/2} \pmod p$. Since a is a quadratic residue, $a^{(p-1)/2} \equiv 1 \pmod p$, hence $a^{(p-1)/4} \equiv \pm 1 \pmod p$. But then $\pm a^{(p+3)/4} \equiv a \pmod p$.

Question 5. Show there are infinitely many primes of the form $4k+1$.

Suppose there are finitely many such primes, say, $p_1, p_2, \ldots, p_k$. Consider $N = 4(p_1 \cdots p_k)^2 + 1$, and let q be a prime divisor of N. Then $q \neq p_i$ for any i, but $N \equiv 0 \pmod q$; hence, $4(p_1 \cdots p_k)^2 \equiv -1 \pmod p$. Therefore, $(-1 \mid q) = 1$ which implies $q \equiv 1 \pmod 4$, a contradiction. Therefore, there are infinitely primes which are 1 modulo 4.

Question 6. Show there are infinitely many primes of the following forms **(a)** $8k+3$, **(b)** $8k+5$, and **(c)** $8k+7$. [Hint: For each part, assume there are only finitely many primes $p_1, p_2, \ldots, p_k$ of the required form. For (a), consider $(p_1 \cdots p_k)^2 + 2$; for (b), consider $(p_1 \cdots p_k)^2 + 4$; for (c), consider $(4p_1 \cdots p_k)^2 - 2$. Use what you know about $(-1 \mid p)$ and $(2 \mid p)$.]

(a) Let $N = (p_1 \cdots p_k)^2 + 2$; then $N \equiv 3 \pmod 8$. Note that the product of two integers which are 1 mod 8 is again 1 mod 8. Therefore, N has an odd prime divisor $q \not\equiv 1 \pmod 8$. Since $N \equiv 0 \pmod q$, we have that $(p_1 \cdots p_k)^2 \equiv -2 \pmod q$, hence $(-2 \mid q) = 1$. Therefore, $q \equiv 1$ or $3 \pmod 8$. But we have excluded the case $q \equiv 1 \pmod 8$. But we easily see that $q \neq p_i$ for all i. We have, therefore, reached a contradiction.

(b) Let $N = (p_1 \cdots p_k)^2 + 4$; then $N \equiv 5 \pmod 8$. As before, there is an odd prime divisor $q \not\equiv 1 \pmod 8$ and $q \neq p_i$ for any i. But then $(p_1 \cdots p_k)^2 \equiv -4 \pmod q$. Since 4 is a quadratic residue, so -1 must also be a quadratic residue. Hence $q \equiv 1 \pmod 4$. But $q \not\equiv 1 \pmod 8$, hence $q \equiv 5 \pmod 8$. We have reached our contradiction.

(c) Let $N = (4p_1 \cdots p_k)^2 - 2$. Then $N/2 \equiv 7 \pmod 8$. and must have an odd prime divisor $q \not\equiv 1 \pmod 8$. We have that $2 \equiv (4p_1 \cdots p_k)^2 \pmod q$, so $(2 \mid q) = 1$ and $q \equiv \pm 1 \pmod 8$. Hence, $q \equiv -1 \pmod 8$, and we again reach a contradiction.

Question 7. Show the following. **(a)** If $p = 4k + 1$ is a prime, then there is an integer x such that $mp = 1 + x^2$ where $0 < m < p$. **(b)** If p is an odd prime, then there are integers x and y such that $1 + x^2 + y^2 = mp$ where again $0 < m < p$.

(a) Since $p \equiv 1 \pmod 4$, we know that -1 is a quadratic residue of p and hence is one of $1^2, 2^2, \ldots, [(p-1)/2]^2$, say, x^2. But, $0 < 1 + x^2 < 1 + (p/2)^2 < p^2$.

(b) The $(p+1)/2$ numbers $x : 0 \leqq x \leqq (p-1)/2$ are incongruent. Also, the $(p+1)/2$ numbers $-1 - y^2 : 0 \leqq y \leqq (p-1)/2$ are incongruent. The cardinalities of these two sets sum to $p+1$; as there are only p residues modulo p, one must reside in both sets. Additionally, $0 < 1 + x^2 + y^2 < 1 + 2(p/2)^2 < p^2$.

Question 8. Determine those primes for which 7 is a quadratic residue.

By quadratic reciprocity, we have that $(7 \mid p) = (-1)^{(p-1)/2}(p \mid 7)$. Suppose first that $p \equiv 1 \pmod 4$: if $p \equiv 1 \pmod 7$, then $p \equiv 1 \pmod{28}$; if $p \equiv 2 \pmod 7$, then $p \equiv 9 \pmod{28}$; if $p \equiv 4 \pmod 7$, then $p \equiv -3 \pmod{28}$. Suppose next that $p \equiv 3 \pmod 4$: if $p \equiv 3 \pmod 7$, then $p \equiv 3 \pmod{28}$; if $p \equiv 5 \pmod 7$, then $p \equiv -9 \pmod{28}$; if $p \equiv 6 \pmod 7$, then $p \equiv -1 \pmod{28}$. We have, therefore, shown the following

$$\left(\frac{7}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1,\ \pm 3,\ \pm 9 \pmod{28}, \\ -1 & \text{if } p \equiv \pm 5,\ \pm 7,\ \pm 11,\ \pm 13 \pmod{28}. \end{cases}$$

Let a and n be positive integers with n odd, and let $n = p_1^{e_1} \cdots p_k^{e_k}$ be the prime power factorization of n. The Jocabi symbol is defined as $(a \mid n) = (a \mid p_1)^{e_1} \cdots (a \mid p_k)^{e_k}$.

Question 9. Prove the following properties of the Jacobi symbol. **(a)** If $a \equiv b \pmod n$, then $(a \mid n) = (b \mid n)$; **(b)** $(ab \mid n) = (a \mid n)(b \mid n)$; **(c)** $(-1 \mid n) = (-1)^{(n-1)/2}$; **(d)** $(2 \mid n) = (-1)^{(n^2-1)/8}$. [Hint: Use the fact that $(1 + (x-1))(1 + (y-1)) = xy$.]

(a) We know that if $a \equiv b \pmod p$, then $(a \mid p) = (b \mid p)$. Hence,

$$\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right)^{e_i} = \prod_i \left(\frac{b}{p_i}\right)^{e_i} = \left(\frac{b}{n}\right).$$

(b) By the totally multiplicative property of the Legendre symbol, we have

$$\left(\frac{ab}{n}\right) = \prod_i \left(\frac{ab}{p_i}\right)^{e_i} = \prod_i \left(\frac{a}{p_i}\right)^{e_i} \left(\frac{b}{p_i}\right)^{e_i} = \left(\prod_i \left(\frac{a}{p_i}\right)^{e_i}\right) \left(\prod_i \left(\frac{b}{p_i}\right)^{e_i}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$

(c) We have

$$\left(\frac{-1}{n}\right) = \prod_i \left(\frac{-1}{p_i}\right)^{e_i} = (-1)^{\frac{1}{2}\sum_i (p_i - 1)e_i}.$$

An obvious induction using the hint implies that $n = \prod_i (1 + (p_i - 1))^{e_i}$. Furthermore, $(1 + (p_i - 1))^{e_i} \equiv 1 + e_i(p_i - 1) \pmod 4$ and $(1 + (p_i - 1))^{e_i}(1 + (p_j - 1))^{e_j} \equiv 1 + e_i(p_i - 1) + e_j(p_j - 1) \pmod 4$. Another clear induction shows $n = \prod_i (1 + (p_i - 1))^{e_i} \equiv 1 + \sum_i e_i(p_i - 1) \pmod 4$. Since then $(n - 1)/2 \equiv \sum_i e_i(p_i - 1)/2 \pmod 2$, the result now follows.

(d) Similar reasoning as that used in part (c) yields

$$\left(\frac{2}{n}\right) = (-1)^{\frac{1}{8}\sum_i e_i(p_i^2 - 1)}.$$

As before, $n^2 \equiv 1 + \sum_i e_i(p_i^2 - 1) \pmod 4$. The result follows as above.

Question 10. Prove quadratic reciprocity holds for the Jacobi symbol, i.e., $(n \mid m)(m \mid n) = (-1)^{(m-1)(n-1)/4}$.

Let $n = \prod_{i=1}^{s} p_i^{e_i}$ and $m = \prod_{i=1}^{t} q_i^{f_i}$. By the definition of the Jacobi symbol and the total multiplicativity of the Legendre symbol,

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{s}\prod_{j=1}^{t}\left[\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right]^{e_i f_j}.$$

Quadratic reciprocity now gives

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{s}\prod_{j=1}^{t}(-1)^{(p_i-1)(q_j-1)e_i f_j/4} = (-1)^{\sum_{i=1}^{s}\sum_{j=1}^{t} e_i \frac{p_i-1}{2} f_j \frac{q_j-1}{2}} = (-1)^{(\sum_{i=1}^{s} e_i \frac{p_i-1}{2})(\sum_{j=1}^{t} f_j \frac{q_j-1}{2})}.$$

As in question 9, we have that

$$\sum_{i=1}^{s} e_i \frac{p_i - 1}{2} \equiv \frac{n-1}{2} \pmod 2,$$
$$\sum_{j=1}^{t} f_j \frac{q_j - 1}{2} \equiv \frac{m-1}{2} \pmod 2.$$

Therefore,

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{(n-1)(m-1)/4}.$$