Math 320 — Number Theory – Final Exam
Tuesday, April 22, 2008.

($\frac{10}{100}$) 1. Compute the Legendre symbol $\left(\frac{43}{73}\right)$.

Solution:

$$\left(\frac{43}{73}\right) = \left(\frac{73}{43}\right) \quad \text{by Quadratic Reciprocity, because } 73 \underset{4}{\equiv} 1,$$
$$\underset{(\diamond)}{=} \left(\frac{30}{43}\right) = \left(\frac{2\cdot 3\cdot 5}{43}\right)$$
$$\underset{(\dagger)}{=} \left(\frac{2}{43}\right)\cdot\left(\frac{3}{43}\right)\cdot\left(\frac{5}{43}\right) \underset{(*)}{=} (-1)\cdot(-1)\cdot(-1) = \boxed{\text{-1}}.$$

Here, $(\diamond)$ is because $73 \underset{43}{\equiv} 30$, and $(\dagger)$ is by by Theorem 7.5. Finally, $(*)$ is because

$$\left(\frac{3}{43}\right) \underset{(1)}{=} -\left(\frac{43}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$
$$\text{while } \left(\frac{5}{43}\right) \underset{(2)}{=} \left(\frac{43}{5}\right) = \left(\frac{3}{5}\right) \underset{(2)}{=} \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) \underset{(3)}{=} -1,$$
$$\text{and } \left(\frac{2}{43}\right) \underset{(4)}{=} -1.$$

Here (1) is by Quadratic Reciprocity because $43 \underset{4}{\equiv} 3$, while (2) is by Quadratic Reciprocity because $5 \underset{4}{\equiv} 1$. Finally, (3) is by Corollary 7.10, because $3 \underset{8}{\not\equiv} \pm 1$. Finally (4) is by Corollary 7.10, because $43 \underset{8}{\not\equiv} \pm 1$. □

($\frac{15}{100}$) 2. Let $p > 3$ be prime. Note that $p \underset{6}{\equiv} \pm 1$ (these are the only values coprime to 6).

(a) Show that

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if} \quad p \underset{6}{\equiv} 1; \\ -1 & \text{if} \quad p \underset{6}{\equiv} -1. \end{cases}$$

Solution:

$$\left(\frac{-3}{p}\right) \underset{(*)}{=} \left(\frac{-1}{p}\right)\cdot\left(\frac{3}{p}\right) \underset{(\dagger)}{=} \begin{cases} 1\cdot 1 & \text{if} \quad p \underset{12}{\equiv} 1, \text{ and hence, } p \underset{4}{\equiv} 1; \\ -1\cdot 1 & \text{if} \quad p \underset{12}{\equiv} -1, \text{ and hence, } p \underset{4}{\equiv} -1; \\ 1\cdot(-1) & \text{if} \quad p \underset{12}{\equiv} 5, \text{ and hence, } p \underset{4}{\equiv} 1; \\ -1\cdot(-1) & \text{if} \quad p \underset{12}{\equiv} -5, \text{ and hence, } p \underset{4}{\equiv} -1. \end{cases}$$
$$= \begin{cases} 1 & \text{if} \quad p \underset{12}{\equiv} 1 \text{ or } -5; \\ -1 & \text{if} \quad p \underset{12}{\equiv} -1 \text{ or } 5. \end{cases} = \begin{cases} 1 & \text{if} \quad p \underset{12}{\equiv} 1 \text{ or } 7; \\ -1 & \text{if} \quad p \underset{12}{\equiv} -1 \text{ or } -7. \end{cases}$$
$$= \begin{cases} 1 & \text{if} \quad p \underset{6}{\equiv} 1; \\ -1 & \text{if} \quad p \underset{6}{\equiv} -1, \end{cases}$$

as desired. Here, $(*)$ is by Theorem 7.5, while $(\dagger)$ is because Corollary 7.7 (p.126) says that

$$\left(\frac{-1}{p}\right) \quad = \quad \begin{cases} 1 & \text{if} \quad p \equiv_4 1; \\ -1 & \text{if} \quad p \equiv_4 -1. \end{cases}$$

while Example 7.10 (p.131) says that $\left(\frac{3}{p}\right) \quad = \quad \begin{cases} 1 & \text{if} \quad p \equiv_{12} \pm 1; \\ -1 & \text{if} \quad p \equiv_{12} \pm 5. \end{cases}$ □

($\frac{15}{100}$) (b) Let $\mathbb{P}_1 := \left\{ p \in \mathbb{P} \; ; \; p \equiv_6 1 \right\}$. Use (a) to show that $\mathbb{P}_1$ is infinite.

Solution: Suppose $\mathbb{P}_1 = \{p_1, \ldots, p_R\}$ is finite, let $N := (2p_1p_2 \cdots p_R)^2 + 3$, and let $M = 2p_1p_2 \cdots p_R$. Then $M^2 = N - 3 \equiv_N -3$. Thus, if p is any prime divisor of N, then $M^2 \equiv_p -3$; hence -3 is a quadratic residue, mod p, so that $\left(\frac{-3}{p}\right) = 1$. Now, N is odd, so p must be odd, which means we can apply part (a) to conclude that $p \equiv_6 1$. In other words, $p \in \mathbb{P}_1$. But for any $r \in [1...R]$, we must have $p \neq p_r$ because $p_r \not| N$ because $N \equiv_{p_r} 3$. Thus, p is an element of $\mathbb{P}_1$ which is *not* in the list $\{p_1, \ldots, p_R\}$, contradicting the hypothesis that $\mathbb{P}_1 = \{p_1, \ldots, p_R\}$. By contradiction, $\mathbb{P}_1$ must be infinite. □

3. Let $n \in \mathbb{N}$, and suppose there is some $a \in \mathbb{N}$ such that $\text{order}_n(a) = n - 1$. Show that n ($\frac{10}{100}$) must be prime.

Solution: For any $a \in \mathbb{N}$, we know that $\text{order}_n(a) \leq \phi(n)$ because $a^{\phi(n)} \equiv_n 1$ by Euler's theorem. Thus, if $\text{order}_n(a) = n - 1$, then $n - 1 \leq \phi(n)$. On the other hand, we know that $\phi(n) := \#\{u \in [1...n) \; ; \; u \perp n\} \leq \#[1...n) \; = \; n - 1$. Thus, we must have $\phi(n) = n - 1$. But this means that *every* number in $[1...n)$ is coprime to n, which means that n is prime. □

($\frac{20}{100}$) 4. Let $M, N \in \mathbb{N}$. Show that $\phi(M)\,\phi(N) = \phi\left[\gcd(M, N)\right] \cdot \phi\left[\text{lcm}(M, N)\right]$.

Solution: Let $D := \gcd(M, N)$ and $L := \text{lcm}(M, N)$. Let $\{p_1, p_2, \ldots, p_R\}$ be the set of all prime factors of either M and N. By arranging these in a suitable order, we can write $M = p_1^{m_1}p_2^{m_2} \cdots p_Q^{m_Q}$ and $N = p_S^{n_S}p_2^{n_2} \cdots p_R^{n_R}$, where $m_1, \ldots, m_Q > 0$ and $n_S, \ldots, n_R > 0$, and where $1 \leq S \leq Q \leq R$. Then we have the following:

$$M \quad = \quad \prod_{r=1}^{Q} p_r^{m_r}, \quad \text{so} \quad \phi(M) \quad = \quad \prod_{r=1}^{Q} p_r^{m_r - 1}(p_r - 1); \tag{1}$$

$$N \quad = \quad \prod_{r=S}^{R} p_r^{n_r}, \quad \text{so} \quad \phi(N) \quad = \quad \prod_{r=S}^{R} p_r^{n_r - 1}(p_r - 1). \tag{2}$$

$$\text{Thus,} \quad \phi(M)\,\phi(N) \quad \underset{(1,2)}{=} \quad \prod_{r=1}^{S-1} p_r^{m_r - 1}(p_r - 1) \cdot \prod_{r=S}^{Q} p_r^{m_r + n_r - 2}(p_r - 1)^2 \cdot \prod_{r=Q+1}^{R} p_r^{n_r - 1}(p_r - 1). \tag{3}$$

$$\text{Meanwhile,} \quad D \quad = \quad \prod_{r=S}^{Q} p_r^{d_r}, \quad \text{where } d_r := \min\{m_r, n_r\}, \text{ for all } r \in [S...Q],$$

$$\text{so that} \quad \phi(D) \quad = \quad \prod_{r=S}^{Q} p_r^{d_r - 1}(p_r - 1), \tag{4}$$

$$\text{and } L = \prod_{r=1}^{S-1} p_r^{m_r} \cdot \prod_{r=S}^{Q} p_r^{\ell_r} \cdot \prod_{r=Q+1}^{R} p_r^{n_r}, \quad \text{where } \ell_r := \max\{m_r, n_r\}, \text{ for all } r \in [S...Q],$$

$$\text{so that } \phi(L) = \prod_{r=1}^{S-1} p_r^{m_r-1}(p_r-1) \cdot \prod_{r=S}^{Q} p_r^{\ell_r-1}(p_r-1) \cdot \prod_{r=Q+1}^{R} p_r^{n_r-1}(p_r-1). \tag{5}$$

$$\begin{aligned}
\text{Thus, } \phi(D)\phi(L) &\underset{(4,5)}{=\!=} \prod_{r=1}^{S-1} p_r^{m_r-1}(p_r-1) \cdot \prod_{r=S}^{Q} p_r^{d_r-1}(p_r-1)p_r^{\ell_r-1}(p_r-1) \cdot \prod_{r=Q+1}^{R} p_r^{n_r-1}(p_r-1) \\
&= \prod_{r=1}^{S-1} p_r^{m_r-1}(p_r-1) \cdot \prod_{r=S}^{Q} p_r^{d_r+\ell_r-2}(p_r-1)^2 \cdot \prod_{r=Q+1}^{R} p_r^{n_r-1}(p_r-1) \\
&= \prod_{r=1}^{S-1} p_r^{m_r-1}(p_r-1) \cdot \prod_{r=S}^{Q} p_r^{m_r+n_r-2}(p_r-1)^2 \cdot \prod_{r=Q+1}^{R} p_r^{n_r-1}(p_r-1) \\
&\underset{(3)}{=\!=} \phi(M)\,\phi(N),
\end{aligned}$$

as desired. □

($\frac{15}{100}$) 5. Suppose $m, n \in \mathbb{N}$ are coprime. Show that $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$.

Solution: We have

$$\begin{aligned}
m^{\phi(n)} + n^{\phi(m)} &\underset{n}{\equiv} m^{\phi(n)} + 0^{\phi(m)} \underset{n}{\equiv} m^{\phi(n)} \overset{(*)}{\underset{n}{\equiv}} 1. \\
m^{\phi(n)} + n^{\phi(m)} &\underset{m}{\equiv} 0^{\phi(n)} + n^{\phi(m)} \underset{m}{\equiv} n^{\phi(m)} \overset{(*)}{\underset{m}{\equiv}} 1. \\
\text{Thus, } m^{\phi(n)} + n^{\phi(m)} &\underset{mn}{\equiv} 1, \text{ by the Chinese Remainder Theorem.}
\end{aligned}$$

Here, both $(*)$ congruences are by Euler's theorem. □

6. For any $s \in (1, \infty)$, let $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$ (the Riemann zeta function). For any $n \in \mathbb{N}$, let

($\frac{15}{100}$) $\tau(n) := \#\{d \in [1...n] \; ; \; d \text{ divides } n\}$. Show that

$$\sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} = \zeta(s)^2.$$

Solution: Let $u(n) := 1$ for all $n \in \mathbb{N}$; then $\zeta(s) = \sum_{n=1}^{\infty} \frac{u(n)}{n^s}$. Thus,

$$\zeta(s)^2 = \left(\sum_{n=1}^{\infty} \frac{u(n)}{n^s}\right) \cdot \left(\sum_{n=1}^{\infty} \frac{u(n)}{n^s}\right) \underset{(*)}{=\!=} \sum_{n=1}^{\infty} \frac{u * u(n)}{n^s} \underset{(\dagger)}{=\!=} \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}$$

Here, $(*)$ is by Theorem 9.6 (p.180), and $(\dagger)$ is because

$$u * u(n) := \sum_{d|n} u(d) \cdot u(n/d) = \sum_{d|n} 1 = \#\{d \in [1...n] \; ; \; d|n\} = \tau(n).$$

□