Math 465 Number Theory, Spring 2025, Solutions 10

1. (i) Prove that if $p \neq 2$, then $\left(\frac{-5}{p}\right)_L = 1$ iff $p \equiv 1, 3, 7$ or $9 \pmod{20}$. (ii) List those $n \leq 25$ for which $x^2 + 5y^2 = n$ is soluble in integers x and y. Are there any primes of the form $p \equiv 1, 3, 7$ or $9 \pmod{20}$ for which $x^2 + 5y^2 = p$ is insoluble in x and y? Which of them are represented by $2x^2 + 2xy + 3y^2$?

$\left(\frac{-5}{p}\right)_L = (-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right)_L$ and both factors are $+1$ when $p \equiv 1 \pmod 4$ and $p \equiv 1$ or $4 \pmod 5$, and both -1 when $p \equiv 3 \pmod 4$ and $p \equiv 2$ or $3 \pmod 5$. (ii) $0, 1, 4, 5, 6, 9, 14, 16, 21, 24, 25$. $3, 7, 23$ are not represented, but are represented by $2x^2 + 2xy + 3y^2$, 3 with $x, y = 0, 1$, 7 with $x, y = 1, 1$, 23 with $x, y = -1, 3$.

2. Prove that the number $n = 2^k \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1$ cannot be represented by the sum of fewer than $2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2$ positive k-th powers.

We have $n < 3^k$ so $n = x2^k + y1^k$, whence $y = n - x2^k$. Thus $x + y = n - x(2^k - 1)$ and thus $x + y$ will be minimal when x is maximal. Since $n = 2^k \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1 < 2^k \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor$, the largest that x can be is $\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1$, and then $y = 2^k - 1$.

3. (i) Show $\sum_{\ell|(m,n)} \mu(\ell)$ is 1 when $(m, n) = 1$ and is 0 otherwise. (ii) Prove $\sum_{m=1,(m,n)=1}^{n} m = \frac{1}{2} n\phi(n)$ when $n > 1$. (iii) Let $N(n, h)$ be the number of m with $1 \leq m \leq n$ and $\big(m(m + h), n\big) = 1$. Prove that $N(n, h) = n \sum_{\ell|n} \frac{\mu(\ell)}{\ell} \rho(\ell)$ where $\rho(\ell)$ is the number of m with $1 \leq m \leq \ell$ and $\ell | m(m+h)$. (iv) Prove that $\rho(\ell)$ is multiplicative. (v) Evaluate $\rho(p)$ and deduce that $N(n, h) = \phi(n) \prod_{p|n, p\nmid h} \frac{p-2}{p-1}$.

(i) This is immediate by Theorem 7.4. (ii) The sum in question is

$$\sum_{m=1}^{n} m \sum_{\ell|(n,m)} \mu(\ell) = \sum_{\ell|n} \mu(\ell) \sum_{m=1,\ell|m}^{n} m = \sum_{\ell|n} \mu(\ell)\ell \sum_{k=1}^{n/\ell} k = \sum_{\ell|n} \mu(\ell)\ell \frac{n}{2\ell} \left(\frac{n}{\ell} + 1\right) =$$

$\frac{n^2}{2} \sum_{\ell|n} \frac{\mu(\ell)}{\ell} + \frac{n}{2} \sum_{\ell|n} \mu(\ell)$. Here the second sum is 0 by Theorem 7.4, and the first is $\frac{1}{2} n\phi(n)$ by Theorem 7.7. (iii) By (i) $N(n, h) = \sum_{m=1}^{n} \sum_{\ell|(m(m+h),n)} \mu(\ell) = \sum_{\ell|n} \mu(\ell) \sum_{m=1,\ell|m(m+h)}^{n} 1$. The inner sum here is $(n/\ell)\rho(\ell)$. (iv) If $\ell = \ell_1\ell_2$ with $(\ell_1, \ell_2) = 1$, then $m_1\ell_2 + m_2\ell_1$ runs over a complete set of residues modulo $\ell_1\ell_2$ as m_1 and m_2 do modulo ℓ_1 and ℓ_2 do respectively. (v) $\rho(p) = 1$ when $p|h$ since then $p|m(m + h)$ implies $p|m$. When $p \nmid h$, then there are two possibilities for m, namely $m \equiv 0$ and $m \equiv -h \pmod p$, so in this case $\rho(p) = 2$. Hence bu (iii) $N(n, h) = n \prod_{p|(n,h)} \frac{p-1}{p} \prod_{p|n, pnmidh} \frac{p-2}{p}$. The conclusion follows from Theorem 7.7.

4. Show that if n is a natural number, then $\prod_{m|n} m = n^{\frac{1}{2}d(n)}$.

When $m|n$ the mapping $m \leftrightarrow \frac{n}{m}$ is a bijection. Thus

$$\Big(\prod_{m|n} m\Big)^2 = \prod_{m|n} m \prod_{m|n} \frac{n}{m} = \prod_{m|n} n = n^{d(n)}.$$