Recall the following notation that we’ve seen before:

- $e_0(n) = n^0 = 1$ is the constant function.
- $\tau(n)$ is the number of divisors of $n$.
- $\omega(n)$ is the number of distinct prime factors of $n$.
- $s(n)$ is the indicator function of perfect squares: $s(n) = 1$ if $n$ is a perfect square, and $s(n) = 0$ otherwise. Recall that $s(n)$ is multiplicative.

1. Find a multiplicative function $f(n)$ such that $\tau(n) = (f * s)(n)$. **Hint:** Start computing the values of $f(1)$, $f(p)$, $f(p^2)$, $f(p^3)$, . . . . There should be a nice way of writing $f(n)$ in terms of $\omega(n)$.

If $f(n)$ is multiplicative, then automatically $f(1) = 1$. Let’s compute $f(p^\alpha)$ for prime powers $p^\alpha$.

We have:

\[
\begin{align*}
2 &= \tau(p) = f(p)s(1) + f(1)s(p) = f(p) + 0 \\
3 &= \tau(p^2) = f(p^2)s(1) + f(p)s(p) + f(1)s(p^2) = f(p^2) + 1 \\
4 &= \tau(p^3) = f(p^3)s(1) + f(p^2)s(p) + f(p)s(p^2) + f(1)s(p^3) = f(p^3) + 2 \\
5 &= \tau(p^4) = f(p^4)s(1) + f(p^3)s(p) + f(p^2)s(p^2) + f(p)s(p^3) + f(1)s(p^4) \\
&\quad = f(p^4) + 2 + 1 \\
&\implies f(p^4) = 2,
\end{align*}
\]

which strongly suggests that $f(p^\alpha) = 2$ for all prime powers. Indeed, we can check that

\[
\left(\sum_{j=0}^{\alpha-1} 2s(p^j)\right) + 1s(p^\alpha) = 2\#\{0 \leq j \leq \alpha - 1: j \text{ is even}\} + \begin{cases} 1, & \text{if } \alpha \text{ is even} \\ 0, & \text{if } \alpha \text{ is odd} \end{cases} = \alpha + 1
\]

for all $\alpha \geq 1$, which proves the pattern found above. Since $f(n)$ is multiplicative, we conclude that

\[
f(n) = \prod_{p^\alpha \mid n} f(p^\alpha) = \prod_{p \mid n} 2 = 2^\omega(n).
\]

2. Define $N(n)$ to be the number of solutions of the congruence $x^2 \equiv -1 \pmod{n}$. Recall that $N(n)$ is a multiplicative function, by the Chinese remainder theorem.

(a) Write down all the values of $N(p^\alpha)$.
(b) Define $G(n) = (N * s)(n)$. Find a formula for $G(n)$.
(c) Find a function $g(n)$ such that $G(n) = (g * e_0)(n)$.
(d) Show that

\[
G(n) = \#\{d \mid n: d \equiv 1 \pmod{4}\} - \#\{d \mid n: d \equiv 3 \pmod{4}\}.
\]

(a) The answer depends on the congruence class of $p$ modulo 4.

(i) When $p \equiv 1 \pmod{4}$, we know that $-1$ is a quadratic residue modulo $p$, and so $x^2 \equiv -1 \pmod{p}$ has two solutions. It’s easy to check that these solutions are nonsingular, and so by Hensel’s lemma, there are two solutions modulo every power of $p$. In other words, $N(p^\alpha) = 2$ when $p \equiv 1 \pmod{4}$. 
(ii) When \( p \equiv 3 \) (mod 4), we know that \(-1\) is a quadratic nonresidue modulo \( p \), and so \( x^2 \equiv -1 \) (mod \( p \)) has no solutions. This implies that there are no solutions modulo any multiple of \( p \) either. In other words, \( N(p^\alpha) = 0 \) when \( p \equiv 3 \) (mod 4).

(iii) When \( p = 2 \), we check by hand that \( x^2 \equiv -1 \) (mod 2) has one solution and \( x^2 \equiv -1 \) (mod 4) has no solutions. This implies that there are no solutions modulo any multiple of 4 either. In other words, \( N(2) = 1 \), while \( N(2^\alpha) = 0 \) for all \( \alpha \geq 2 \).

(b) The function \( N(n) \) is multiplicative by the Chinese remainder theorem (since it counts the roots of the polynomial \( x^2 + 1 \) modulo \( n \)). Since \( N(n) \) and \( s(n) \) are both multiplicative, their convolution \( G \) must be multiplicative as well, and so it suffices to calculate \( G(n) \) on prime powers.

(i) When \( p \equiv 1 \) (mod 4), we have \((G * s)(p^\alpha) = (\sum_{j=0}^{\alpha-1} 2s(p^j)) + 1s(p^\alpha)\); we did this calculation in problem #1 above, and the answer is \( \alpha + 1 \). (In other words, on these primes \( N \) “acts like” \( 2\omega(n) \), and so \( G \) “acts like” \( 2\omega(n) * s(n) = \tau(n) \) on these primes.)

(ii) When \( p \equiv 3 \) (mod 4), we have \((G * s)(p^\alpha) = (\sum_{j=0}^{\alpha-1} 0s(p^j)) + 1s(p^\alpha) = s(p^\alpha)\), which equals 1 if \( \alpha \) is even and 0 if \( \alpha \) is odd. (In other words, on these primes \( N \) “acts like” \( \iota(n) \), and so \( G \) “acts like” \( (\iota * s)(n) = s(n) \) on these primes.)

(iii) When \( p = 2 \), we have \((G * s)(p^\alpha) = (\sum_{j=0}^{\alpha-2} 0s(p^j)) + 1s(p^\alpha-1) + 1s(p^\alpha) = 1 \), since exactly one of \( \alpha - 1 \) and \( \alpha \) is even. (In other words, on these primes \( N \) “acts like” \( \mu^2(n) \), and so by an example we did in class, \( G \) “acts like” \( (\mu^2 * s)(n) = e_0(n) \) on these primes.)

(c) By the Möbius inversion formula, \( G(n) = (g * e_0)(n) \) if and only if \( g(n) = (G * \mu)(n) \). Since both \( G(n) \) and \( \mu(n) \) are multiplicative functions, so is \( g(n) \), and it suffices to calculate \( g(p^\alpha) \) for prime powers \( p^\alpha \). In all cases, note that

\[
(G * \mu)(p^\alpha) = \left(\sum_{j=0}^{\alpha-2} 0G(p^j)\right) + (-1)G(p^{\alpha-1}) + 1G(p^\alpha) = G(p^\alpha) - G(p^{\alpha-1}).
\]

(i) When \( p \equiv 1 \) (mod 4), we have \( g(p^\alpha) = G(p^\alpha) - G(p^{\alpha-1}) = (\alpha + 1) - \alpha = 1 \). (In other words, on these primes \( G \) “acts like” \( \tau \), and so \( g \) “acts like” \( \tau * \mu = (e_0 * e_0) * \mu = e_0 * (e_0 * \mu) = e_0 * \iota = e_0 \) on these primes.)

(ii) When \( p \equiv 3 \) (mod 4), we have \( g(p^\alpha) = G(p^\alpha) - G(p^{\alpha-1}) \), which equals 1 if \( \alpha \) is even and \(-1 \) if \( \alpha \) is odd. (We haven’t seen this function before.)

(iii) When \( p = 2 \), we have \( g(p^\alpha) = G(p^\alpha) - G(p^{\alpha-1}) = 1 - 1 = 0 \). (In other words, on these primes \( G \) “acts like” \( e_0(n) \), and so \( g \) “acts like” \( (e_0 * \mu)(n) = \iota(n) \) on these primes.)

Note in particular that \( g(p^\alpha) \) equals 1 if \( p^\alpha \equiv 1 \) (mod 4), equals \(-1 \) if \( p^\alpha \equiv 3 \) (mod 4), and equals 0 if \( p^\alpha \) is even. We can now check that these descriptions play well with multiplicativity, so that \( g(n) \) itself equals 1 if \( n \equiv 1 \) (mod 4), equals \(-1 \) if \( n \equiv 3 \) (mod 4), and equals 0 if \( n \) is even.
(d) From part (c),

$$G(n) = (g \ast e_0)(n) = \sum_{d \mid n} g(d)$$

$$= \sum_{d \mid n} \begin{cases} 
1, & \text{if } d \equiv 1 \pmod{4}, \\
-1, & \text{if } d \equiv 3 \pmod{4}, \\
1, & \text{if } d \text{ is even}
\end{cases}$$

$$= \#\{d \mid n: d \equiv 1 \pmod{4}\} - \#\{d \mid n: d \equiv 3 \pmod{4}\}$$

as claimed. [One interesting side note: from its description in part (c), it’s obvious that $G(n)$ takes only nonnegative values. That’s much less obvious from this last formula; indeed, this formula is the (mod 4) analog of the function $\tau_1(n) - \tau_2(n)$ from problem #2 on Homework 7.)

Okay, so why all these funny functions? Theorem 3.21 of Niven, Zuckerman, & Montgomery tells us that the number $r(n)$ of proper representations of the integer $n$ as a sum of two squares is exactly $4N(n)$, where $N(n)$ is as defined in problem #2. (Indeed, we already knew that $r(n)$ is nonzero if and only if $N(n)$ is nonzero, from Group Work #7.) It’s also pretty easy to show that the number $R(n)$ of (not necessarily proper) representations of the integer $n$ as a sum of two squares is equal to $(r \ast s)(n) = 4(N \ast s)(n) = 4G(n)$. (See the proof of Theorem 3.21; in brief, every representation of $n$ as $x^2 + y^2$ corresponds to a proper representation of its divisor $n/d^2$ as $(x/d)^2 + (y/d)^2$, where $d = (x, y)$.) So we have proved a classical result: the number of representations of $n$ as a sum of two squares is equal to the number of divisors of $n$ that are congruent to 1 (mod 4), minus the number of divisors of $n$ that are congruent to 3 (mod 4).