Math 223 Number Theory, Spring ’07
Homework 7 Solutions

(1) If \( p \) is a prime, prove that \( p + 2 \) is a prime if and only if \( 4((p - 1)! + 1) + p \equiv 0 \pmod{p + 2} \). (Hint: Wilson’s Theorem is already and if and only if statement. Hint 2: Do this for \( p = 2 \) separately, and then assume \( p \) is odd.)

**Solution:** First suppose \( p = 2 \). Then \( p + 2 = 4 \) which is not a prime. On the other hand, \( 4((2 - 1)! + 1) + 2 = 10 \not\equiv 0 \pmod{4} \) so the claim is verified for \( p = 2 \). If \( p \) is an odd prime, then

\[
p + 2 \text{ is prime } \iff (p + 1)! \equiv -1 \pmod{p + 2}
\]

\[
\iff (p + 1)p(p - 1)! \equiv -1 \pmod{p + 2}
\]

\[
\iff (-1)(-2)(p - 1)! \equiv -1 \pmod{p + 2}
\]

\[
\iff 2(p - 1)! \equiv -1 \pmod{p + 2}
\]

\[
\iff 4(p - 1)! \equiv -2 \pmod{p + 2}
\]

\[
\iff 4(p - 1)! + 4 \equiv 2 \pmod{p + 2}
\]

\[
\iff 4((p - 1)! + 1) + p \equiv 0 \pmod{p + 2},
\]

where the first equivalence is Wilson’s Theorem.

(2) (14.1) If \( a^n + 1 \) is prime for some integers \( a \geq 2 \) and \( n \geq 1 \), show that \( n \) must be a power of 2.

**Solution:** If \( n \) is not a power of 2, then it can be written as \( n = 2^k m \) for some \( k \in \mathbb{Z} \) and some odd \( m > 1 \). Now, for any positive integer \( b \), recall the formula

\[
(b^m + 1) = (b + 1)(b^{m-1} - b^{m-2} + b^{m-3} - \cdots - b + 1).
\]

(This formula is only true because \( m \) is odd. Do you see why?) Using this with \( b = a^2 \), we get

\[
a^n + 1 = a^{2^k} + 1 = (a^2)^m + 1 = (a^2 + 1)((a^2)^{m-1} - (a^2)^{m-2} + (a^2)^{m-3} - \cdots - (a^2) + 1)
\]

and thus \( a^n + 1 \) cannot be a prime as it is a product of two integers greater than 1.

(3) (14.2) Let \( F_k = 2^{2^k} + 1 \), so, for example, \( F_1 = 5 \), \( F_2 = 17 \), \( F_3 = 257 \), and \( F_4 = 65537 \). Fermat thought that all of the \( F_k \)'s might be prime, but Euler showed in 1732 that \( F_5 \) factors as \( 641 \cdot 6700417 \), and in 1880 Landry showed that \( F_6 \) is also composite. Primes of the form \( F_k \) are called Fermat primes. Show that, if \( k \neq m \), then the numbers \( F_k \) and \( F_m \) have no common factors; that is, show that \( \gcd(F_k, F_m) = 1 \). (Hint: If \( k > m \), show that \( F_m \) divides \( F_k - 2 \).)

**Solution:** If \( k > m \), then

\[
F_k - 2 = 2^{2^k} - 1 = (2^{2^{k-1}} - 1)(2^{2^{k-1}} + 1)
\]

\[
= (2^{2^{k-2}} - 1)(2^{2^{k-2}} + 1)(2^{2^{k-1}} + 1)
\]

\[
= \cdots
\]

\[
= (2^m - 1)(2^m + 1)\cdots(2^{2^{k-2}} + 1)(2^{2^{k-1}} + 1)
\]

\[
= (2^m - 1)F_m\cdots(2^{2^{k-2}} + 1)(2^{2^{k-1}} + 1).
\]

Thus \( F_m \) divides \( F_k - 2 \). But then \( F_m \) does not divide \( F_k \), since if it did, it would also have to divide \( F_k - (F_k - 2) = 2 \), which is a contradiction. But more is true from this computation: Note that all the factors of \( F_m \) are also factors of \( F_m - 2 \). Then, if \( F_m \) and \( F_k \) had a common factor, this would also have to be a factor of \( F_k - (F_k - 2) = 2 \), i.e. it would have to be 2. But this is impossible as \( F_m \) and \( F_k \) are odd.