MATH 3070
Assignment # 4 Solutions
Due Thursday, October 23, 2008

1. Solution 1:
   Let $n = p_1^{a_1} \cdots p_k^{a_k}$ be the unique factorization of n.
   Then $\varphi(n) = p_1^{a_1-1} \cdots p_k^{a_k-1}(p_1 - 1) \cdots (p_k - 1) = 12 = 2^2 3$, where p_k is the largest prime divisor of n. Then since $p_k - 1$ must divide $\varphi(n) = 12$, the possibilities for $p_k - 1$ are $12, 6, 4, 3, 2, 1$.

   If $p_k - 1 = 12$, then $p_k = 13$ and so $a_k = 1$. All the other $p_i - 1$ factors must be 1 and so $k = 1$ or $k = 2$ with $p_1 = 2$, $a_1 = 1$. This corresponds to $n = 13, 26$.

   If $p_k - 1 = 6$, Then $p_k = 7$ and so $a_k = 1$ in this case as well, as $7 \not| 12$. We only have a factor of 2 in the remaining parts of $\varphi(n)$. Since $5 - 1 = 4 > 2$ we cannot have $p_i = 5$ for any i. So the only possibilities are $p_i = 2$ or 3. If there is a factor $p_i = 3$ then we must have $a_i = 1$, and as before we may insert $p_1 = 2$. So we find $n = 21, 42$. If $p_i \neq 3$ for any i then we must have $k = 2$ and $p_1 = 2$, which forces $a_1 = 2$ and so $n = 28$.

   If $p_k - 1 = 4$ then $p_k = 5$ and $a_k = 1$. But then 3 must divide the remaining factors. Since $p_i \leq 3$ for all $i < k$, $p_i - 1$ is coprime to 3, so we must have a $p_i = 3$, which introduces another factor of 2 from $p_i - 1$. This means there is a factor of 8 in $\varphi(n)$, a contradiction.

   $p_k - 1 = 3$ is impossible, since 4 is not a prime.

   If $p_k - 1 = 2$, then $p_k = 3$, so $a_k = 2$ by the same reasoning as above to obtain the factor of 3 in $\varphi(n)$. This contributes a factor of 6 in $\varphi(n)$. So $k = 2$ and $p_1 = 2$, with $2 = 2^{a_1-1}$ so $a_1 = 2$. This corresponds to $n = 2^2 3^2 = 36$.

   Finally, if $p_k - 1 = 1$ then $k = 1$ and $p_1 = 2$ which means $n = 2^{a_1}$ so $\varphi(n) = 2^{a_1-1}$ is never 12. Thus the entire solution set for n is $\{13, 26, 21, 42, 28, 36\}$.

   Solution 2:
   Let $n = p_1^{a_1} \cdots p_k^{a_k}$ be the unique factorization of n.
   Then $\varphi(n) = p_1^{a_1-1} \cdots p_k^{a_k-1}(p_1 - 1) \cdots (p_k - 1) = 12 = 2^2 3$.
   Since the $p_i - 1$ are increasing, and $12 = 1 \cdot 2 \cdot 2 \cdot 3$, 12 cannot be the product of more than 3 distinct numbers. Thus $k \leq 3$. Now let's look at the various cases and possibilities.

   If $k = 1$, then $12 = p_1^{a_1-1}(p_1 - 1)$ so either $p_1 = 2, p_1 = 3$, or $a_1 = 1$ so $n = p_1$. The first two cases are impossible as $\varphi(2^n) = 2^{n-1} \neq 12$ for any n, and $\varphi(3^n) = 3^{n-1} \cdot 2 \neq 12$ for any n. In the last case, we have $p_1 - 1 = 12$ so $n = p_1 = 13$ works.

   If $k = 2$, then $12 = p_1^{a_1-1} p_2^{a_2-1}(p_1 - 1)(p_2 - 1)$. If neither of the a_i are 1, then this forces $p_1 = 2$ and $p_2 = 3$ so $12 = 2^{a_1-1} 3^{a_2-1}(1)(2)$, so that $a_1 - 1 = a_2 - 1 = 1$ and $n = 2^2 3^2 = 36$.

   If $a_1 = 1$ and $a_2 > 1$ then since $p_2 > p_1 \geq 2$, we must have $p_2 = 3$ and so $a_2 = 2$. This yields $12 = 3(3 - 1)(p_1 - 1) = 6(p_1 - 1)$ so $p_1 - 1 = 2$ and $p_1 = 3$, a contradiction. If $a_2 = 1$ and $a_1 > 1$ then we have two cases: $p_1 = 2$ or $p_1 = 3$. In the first case, we find that either $a_1 = 2$

or $a_1 = 3$, giving $12 = 2(p_2 - 1)$ or $12 = 4(p_2 - 1)$ The first case yields $p_2 = 7$ and the second case is impossible. So we have the solution $n = 28$. If $p_1 = 3$ then we must have $a_1 = 2$ so $12 = 3(2)(p_2 - 1)$, so $p_2 - 1 = 2$ and $p_2 = 3$ is a contradiction.

Finally, if $a_1 = a_2 = 1$ then $n = (p_1 - 1)(p_2 - 1)$, giving the possible $(p_1 - 1, p_2 - 1)$ pairs as $(1, 12), (2, 6)$, and $(3, 4)$. Only the first two yields solutions $n = 26$ and $n = 21$.

If $k = 3$, first note that $p_3 > p_2 > p_1 \geq 2$ so $p_3 \geq 5$ and $p_2 \geq 3$. Therefore $(p_1 - 1)(p_2 - 1)(p_3 - 1) \geq 4 \cdot 2 \cdot 1 = 8$. But that product must be a factor of 12, and the only factor of 12 greater than 8 is 12 itself. Therefore $12 = (p_1 - 1)(p_2 - 1)(p_3 - 1)$ and we must have $a_1 = a_2 = a_3 = 1$. The possible triples $(p_1 - 1, p_2 - 1, p_3 - 1)$ are $(1, 2, 6)$ and $(1, 3, 4)$. Only the first one yields a solution, and it is $n = 2 \cdot 3 \cdot 7 = 42$.

Thus, the list of all n such that $\varphi(n) = 12$ is $\{13, 21, 26, 28, 36, 42\}$

2. We simply need to multiply n by primes that are one more than a power of two. In particular, for $k \geq 2$ we have $\varphi(3 \cdot 2^k) = \varphi(5 \cdot 2^{k-1}) = 2^k$.

3. Obviously $25! \equiv 0 \pmod{23}$. Now $18! = 22!(22^{-1})(21^{-1})(20^{-1})(19^{-1}) \equiv 22![(-1)(-2)(-3)(-4)]^{-1} \equiv 22!(24)^{-1} \pmod{23}$. But $24 \equiv 1 \pmod{23}$ so $22! \equiv 18! \pmod{23}$. Now apply Wilson's Theorem and we find that $18! + 25! \equiv 22! \equiv -1 \pmod{23}$. So the remainder is 22.

4. (a) If $4n^2 + 1$ is divisible by some prime $p \equiv 3 \pmod 4$, then $4n^2 \equiv -1 \pmod p$. Thus -1 would be a quadratic residue mod p. But -1 is a quadratic residue if and only if $p \equiv 1 \pmod 4$. So $4n^2 + 1$ can never have a prime factor congruent to $3 \pmod 4$.

   (b) Suppose not. Let $p_1 < p_2 < \cdots < p_k$ be the list of all primes congruent to $1 \pmod 4$. Let $N = 4(p_1 p_2 \cdots p_k)^2 + 1$. This is odd and obviously greater than p_k. Thus it must be composite. But N is coprime to all the primes congruent to $1 \pmod 4$. Thus all of its prime factors must be congruent to $3 \pmod 4$ (since 2 does not divide N). But this contradicts part a.

5. (a) Since half of the a are quadratic residues and the other half are non-residues, we have the same number of $+1$ and -1 in the sum. So it evaluates to zero.

   (b) Since the Legendre symbol is completely multiplicative, the expression is

$$\prod_{k=1}^{p-1} \left(\frac{k}{p}\right) = \left(\frac{(p-1)!}{p}\right) = \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

6. If $a \equiv x^2 \pmod p$ has a solution, then $(x^{-1})^2 a \equiv (x^{-1})^2 x^2 \equiv 1 \pmod p$ so $(x^{-1})^2 \equiv a^{-1} \pmod p$. Therefore a is a quadratic residue implies a^{-1} is also. The converse follows from switching a with a^{-1} in the above argument.

7. If $p = 2$, then both 3 and 5 are quadratic residues mod p. Now suppose p is an odd prime. By quadratic reciprocity, we have

$$\left(\frac{3}{p}\right) = (-1)^{1(p-1)/2} \left(\frac{p}{3}\right) = (-1)^{(p-1)/2} \left(\frac{p}{3}\right).$$

Now, 1 is the only quadratic residue mod 3 and $(-1)^{(p-1)/2} = 1$ if and only if $p \equiv 1 \pmod 4$. So we have

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

Similarly, we find that

$$\left(\frac{5}{p}\right) = (-1)^{2(p-1)/2}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 5, \\ -1 & \text{if } p \equiv \pm 2 \pmod 5, \end{cases}$$

since p is an odd prime so $(-1)^{p-1} = 1$ always. In fact, since p is odd, we can conclude that

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{10}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{10}. \end{cases}$$

8. We may rewrite the sum as $S := 1^2 + (2^{-1})^2 + \cdots + ((p-1)^{-1})^2$. Now, since we are summing over the inverses of all invertible residue classes mod p, this is just a rearrangement of a sum over all invertible residue classes mod p. Thus

$$S \equiv 1^2 + 2^2 + \cdots + (p-1)^2 \equiv \frac{p(p+1)(2p+1)}{6} \pmod p.$$

Now since $p > 3$ is a prime, $\gcd(6, p) = 1$ so the p does not cancel, and the evaluation must be $0 \pmod p$.