Math 40520 Theory of Number
Homework 4

Due Wednesday 9/16

Do 5.

1. Exercise 2.25 on page 47.
2. Exercise 2.26 on page 47.
3. Exercise 2.33 on page 47. Feel free to use Sage here, but then please include the code.
4. Show that if $m \mid n$ then $\varphi(m) \mid \varphi(n)$.
5. Let n be a number such that $n+1$ is divisible by 24. If $d \mid n$ show that 24 divides $d^2 - 1$.
6. Compute
$$12^{34^{56^{78}}} \mod 90$$
[Hint: It is much easier to use Euler's theorem in conjunction with the Chinese Remainder Theorem.] (The author of this problem was very proud of having used each digit exactly once. This idiosyncrasy actually makes the problem easier.)
7. Let p be a prime number and a an integer coprime to p. Show that $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$ with 1 if and only if there exists b such that $a \equiv b^2 \pmod{p}$.
8. Let $p \equiv 3 \pmod 4$ be a prime number. Suppose you know that $y \equiv x^2 \pmod{p}$ for some $x \in \mathbb{Z}_p^\times$. Show that $x \equiv \pm y^{(p+1)/4} \pmod{p}$.