

# Math 40520 Theory of Number

## Homework 4

Due Wednesday 9/28

**Do 5.**

1. Exercise 2.25 (a) on page 47 but with  $X$  (polynomial variable) instead of 2.
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

$$13^{25^{47^{68}}} \pmod{90}$$

[Hint: It is much easier to use Euler's theorem in conjunction with the Chinese Remainder Theorem.]

7. 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  $x \equiv \pm y^{(p+1)/4} \pmod{p}$  are the only two solutions.
8. Let  $p > 2$  be a prime. Show that the equation  $x^n \equiv a \pmod{p}$  has either 0 or  $(n, p - 1)$  solutions.