MATH 350 ASSIGNMENT 11, SPRING 2017

Due in class on Monday, April 10

Part 1. From the textbook *A friendly introduction to number theory*

- Exercise 36.2 (a), 4th edition (= Exercise 34.2, (a), 3rd edition)
- Exercise 36.3, (a)–(c), 4th edition (= Exercise 34.3, (a)–(c), 3rd edition)
- Exercise 36.5, (a) & (b), 4th edition (= Exercise 34.5, (a) & (b), 3rd edition)

Part 2. Let $n \geq 3$ be an odd positive integer. Let b be an integer relatively prime to n. We say that n passes the *Solovay–Strassen* test by b for primality if

$$b^{(n-1)/2} \equiv \left(\tfrac{b}{n}\right) \pmod{n},$$

where the right hand side of the above formula is the Jacobi symbol.

(a) For $n = 35$, find the number of elements of the following set

$$\{\, \bar{b} \in (\mathbb{Z}/35\mathbb{Z})^{\times} \mid \bar{b}^{(n-1)/2} = \left(\tfrac{b}{n}\right) \bmod n \}$$

(b) Suppose that there exists a prime number p such that $n \equiv 0 \pmod{p^2}$. Show that there exists an integer b relatively prime to n such that n fails the Solovay–Strassen test by b.

Part 3. Extra credit problems.

E1. Continue in the set-up of Part 2.

(c) Suppose that n is a product of $r \geq 2$ distinct odd prime numbers. Show that exists an integer b relatively prime to n such that n fails the Solovay–Strassen test by b. (So there is no analogue of Carmichael number for the Solovay-Strassen test.)

(d) Suppose that n is an odd composite natural number. Prove that

$$\#\{b \in \mathbb{N} \mid 2 \leq b \leq n-1,\ b^{(n-1)/2} \not\equiv \left(\tfrac{b}{n}\right) \pmod{n}\} \geq \tfrac{n-1}{2}$$

E2. Exercise 36.6, 4th edition (= Exercise 34.6, 4th edition)