Hints to some of the practice problems

April, 2005

1. Prove that $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$ for all $n \in \mathbb{N}_{>0}$.
   [Hint: induction]

2. Prove that

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}$$

for all $n \in \mathbb{N}_{>0}$.
   [Hint: induction]

3. Determine whether the following statements are true or false.
(a) For prime numbers p, the Legendre symbol $\left(\frac{5}{p}\right)$ depends only on the congruence class of p modulo 5.
(b) For prime numbers p, the Legendre symbol $\left(\frac{11}{p}\right)$ depends only on the congruence class of p modulo 11.
(c) For non-zero natural numbers a, b which are relatively prime, the Jacobi symbol $\left(\frac{a}{b}\right)$ depends only on the congruence class of a modulo b. (d) For non-zero natural numbers a, b which are relatively prime, the Jacobi symbol $\left(\frac{a}{b}\right)$ depends only on the congruence class of b modulo $4a$.
   [Hint: Use the reciprocity law. For instance, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ depends only on $p \pmod 5$.]

4. Find all integers n such that $-1000 \le n \le 1000$ and satisfying the following three congruence relations

$$n \equiv 2 \pmod 3, \quad n \equiv 3 \pmod 5 \quad \text{and } n \equiv 4 \pmod 7 .$$

   [Hint: The conditions mean that $n \equiv 54 \pmod{105}$.]

5. For $p = 173$ and $p = 401$, determine the set of all elements $x \in \mathbb{Z}/p^2\mathbb{Z}$ such that

$$x^5 \equiv 1 \pmod{p^2} .$$

   [Hint: First try to find all solutions of $x^5 \equiv 1 \pmod p$, then uses Hensel's Lemma.]

6. Determine the set of all $x \in \mathbb{Z}/13^4\mathbb{Z}$ such that $x^3 \equiv -1 \pmod{13^4}$.
   [Hint: First try to find all solutions of $x^3 \equiv -1 \pmod{13}$, then uses Hensel's Lemma.]

7. Let S be the set of all pairs (a, b) with $a, b \in \mathbb{Z}$, $0 \le a, b \le 20$ such that there exists an integer x such that $x \equiv a \pmod{36}$ and $x \equiv b \pmod{100}$. Determine the number of elements of S.
   [Hint: The existence of such an integer x implies that $a \equiv b \pmod 4$.]

8. Let p, q be prime numbers, $p \neq q$. Find a natural number n with $0 \neq n < pq$ such that $p^{2q-1} + q^{2p-1} \equiv n \pmod{pq}$. (The number n should be given in terms of p and q.)

[$p + q$ does it.]

9. Let p be an odd prime number. Show that the Legendre symbol $\left(\frac{7}{p}\right)$ depends only on the congruence class of p modulo 28, and determine the value of $\left(\frac{7}{p}\right)$ for each congruence class of p modulo 28.

[Hint: Use the reciprocity law.]

10. (a) Determine the simple continued fraction expansion of $\frac{\sqrt{7}}{2}$.
(b) Find natural numbers a, b, c, d such that $\frac{c}{d} < \frac{\sqrt{7}}{2} < \frac{a}{b}$, $b, d > 100$, and $ad - bc = 1$.

[Hint: For (b), use suitable convergents of the simple continued fraction expansion of $\frac{\sqrt{7}}{2}$.]

11. Does the quadratic congruence equation

$$x^2 + 2\,x + 1002 \equiv 0 \pmod{483}$$

have a solution in $\mathbb{Z}/483\mathbb{Z}$?

[Hint: The condition is that there exist solutions for $x^2 + 2\,x + 1002 \equiv 0 \pmod{p}$ for $p = 3, 7, 23$.

12. Expand $\frac{173}{409}$ as a simple continued fraction.

13. Find natural numbers a, b such that $a\,409 - b\,250 = 1$.

[Hint: Use the Euclidean algorithm.]

14. Let p be a prime number. Determine the following numbers in terms of p.

(a) the number of quadratic non-residues modulo p,

(b) the number of primitive elements in $(\mathbb{Z}/p\mathbb{Z})^\times$,

(c) the number of non-primitive elements in $(\mathbb{Z}/p\mathbb{Z})^\times$,

(d) the number of elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ which are quadratic non-residues but not primitive.

15. Determine the number of elements of $(\mathbb{Z}/9797\mathbb{Z})^\times$ of order 100.
[Hint: The Chinese Remainder Theorem gives a natural one-to-one correspondence between $(\mathbb{Z}/9797\mathbb{Z})^\times$ and $(\mathbb{Z}/97\mathbb{Z})^\times \times (\mathbb{Z}/101\mathbb{Z})^\times$. The following fact follows as a consequence: For every integer n which is relatively prime to 9797, the order of $n \pmod{9797}$ is equal the least common multiple of the order of $n \pmod{97}$ and the order of $n \pmod{101}$.]

16. (a) What is the maximal possible order for elements of $(\mathbb{Z}/9797\mathbb{Z})^\times$?
(b) Determine the number of elements of $(\mathbb{Z}/9797\mathbb{Z})^\times$ whose order are maximal possible.

17. Prove that 561 is an Euler pseudoprime to the base 2, i.e.

$$2^{280} \equiv \left(\frac{2}{561}\right) \pmod{561},$$

where $\left(\frac{2}{561}\right)$ is the Jacobi symbol.

18. Suppose that n is natural number, $n \equiv 5 \pmod{12}$ and that n is an Euler pseudoprime to the base 3. Prove that n is a strong pseudoprime to the base 3, i.e. n passes the Miller-Rabin test to the base 3.

19. Relate the length of the period of the decimal expansion of $\frac{1}{161}$ to the order of a suitable element in $(\mathbb{Z}/n\mathbb{Z})^\times$ for a suitable integer n, and determine the length of that period.

[The length of the period of the decimal expansion of $\frac{1}{161}$ is equal to the order of the element $10 \pmod{161}$ in $\mathbb{Z}/161\mathbb{Z})^\times$

20. The number 1729 factors as $1729 = 7 \times 13 \times 19$.

(a) Determine the number of elements in $(\mathbb{Z}/1729)^\times$ of order 3.

(b) Determine the number of elements in $(\mathbb{Z}/1729)^\times$ which are squares, i.e. equal to the square of some element in $(\mathbb{Z}/1729)^\times$.

(c) Determine the number of elements in $(\mathbb{Z}/1729)^\times$ which are cubes, i.e. equal to the cube of some element in $(\mathbb{Z}/1729)^\times$.

(c) Determine the number of elements in $(\mathbb{Z}/1729)^\times$ which are fourth powers, i.e. congruent to x^4 modulo 1729 for some integer x.

[See the hint to Problem 15.]