MAT3166: ASSIGNMENT #3

DUE IN CLASS ON WEDNESDAY, NOVEMBER 9, 2011

Part I: Exercises in Number Theory

Sections refer to the textbook, for your information and reference. If you consult an outside source, cite it, and you must close that book/website and write up your solution by yourself, with your own explanations.

1. (4 pts) (Section 4.1) Use Fermat’s little theorem to show that $8^{22} - 3^{22} \equiv 0 \pmod{11}$.

2. (3 pts) (Section 4.3) Suppose that $a^x \equiv 1 \pmod{m}$ and $a^y \equiv 1 \pmod{m}$. Set $g = (x, y)$. Prove that $a^g \equiv 1 \pmod{m}$.

3. (a) (4 pts) (Section 7.1) Suppose $g$ is a primitive root mod $n$ and $n > 2$. So every element of $U_n$ can be written in the form $g^k$ for some integer $0 \leq k < \phi(n)$. Using this, describe the set of all $a \in U_n$ such that $x^2 \equiv a \pmod{n}$ has a solution. Such an $a$ is called a quadratic residue mod $n$.

(b) (5 pts) (Section 7.2) Let $p$ be a prime and $(a, p) = 1$. Show that $x^2 \equiv a \pmod{p}$ has a solution if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

4. (a) (4 pts) Prove that if $a, b \in U_n$ are such that $(\text{ord}_n(a), \text{ord}_n(b)) = 1$ then $\text{ord}_n(ab) = \text{ord}_n(a) \text{ord}_n(b)$.

(b) (4 pts) (Section 7.1) Suppose $p$ is prime and $\text{ord}_p(a) = 3$. Show that $3|(p-1)$ and $1+a+a^2 \equiv 0 \pmod{p}$. (Hint: for the second, multiply the left side by $a$.) Now use these facts to deduce that $\text{ord}_p(a+1) = 6$.

5. (2 pts) (Section 7.3) Suppose $p$ is a prime and $g$ is a primitive root mod $p$. What is the index of $-1$? That is, find $x$ such that $g^x \equiv -1 \pmod{p}$.

6. (2 pts) (Section 5.3) The number $n = 10088821$ factors as $pq$ for distinct primes $p$ and $q$. Given that $\phi(n) = 10082272$, find $p$ and $q$. Hint: $\phi(pq) = (p-1)(q-1)$, so you have two equations with two unknowns and should be able to solve. No points for guesswork/lookup tables/brute force factorization.

Part II: Additional exercises, not to be handed in

Here is a selection of exercises on the material we have covered in the course so far. Some are copied directly from the textbook (for the benefit of those students without a text); section numbers refer to the textbook. (If you don’t have the text then you can compare the section numbers with our website to get a sense of what subject material it relates to.)
Please do not hand in these exercises, although you are very welcome to discuss them with me, via email, in office hours or after class. I won’t post solutions but will be happy to tell you how to solve them.

1. (Section 2.1) Show that a perfect square is never of the form $3k + 2$ for any $k \in \mathbb{Z}$. Conclude that if $p$ is prime and $p \geq 5$ then $p^2 + 2$ is always composite.

2. (Section 2.1) Show that for any prime $p$, $p$ divides the binomial coefficient $\binom{p}{k}$, for $1 \leq k \leq p-1$.

3. (Section 2.1) Show that $6|(n^3 - n)$ for all integers $n$. Does $4|(n^4 - n)$ for all integers $n$?

4. (Section 2.1) Determine all primes of the form $n^3 - 1$.

5. (Section 2.2) Show that the product of primes of the form $p = 4k + 1$ is also of that form. Now let $p_1, \ldots, p_n$ be a finite set of primes and construct $N = 4p_1p_2\cdots p_n + 3$; prove that $N$ has a prime factor of the form $4k + 3$. Deduce from this that there are infinitely many primes of the form $4k + 3$.

6. (Section 2.3) Let $p$ be prime and $a, n$ positive integers. Show that if $p|a^n$ then $p|a$.

7. (Section 2.3) Let $p$ be a prime. Find the sum of all the divisors of $p^n$ for any $n \geq 1$.

8. (Section 2.3) Show that if $ab = m^2$ and $(a, b) = 1$ then $a$ and $b$ are each perfect squares.

9. (Section 2.3) Show that if $n$ has $t$ positive divisors then the product of these divisors is $n^{t/2}$.

10. (Section 2.5) Find $(6963, 7385)$ via (a) Euclidean algorithm and (b) prime factorization. Express $(6963, 7385)$ as a linear combination of 6963 and 7385.

11. (Section 2.5) Prove that if $(a, b) = 1$ then $(a + b, a - b)$ is either 1 or 2.

12. (Section 2.5) Prove or disprove: $(a, b) = 1$ and $(b, c) = 1$ implies $(a, c) = 1$.

13. (Section 2.5) Let $p$ be prime and suppose $p^n|ab$ but $p$ does not divide $a$. Prove that $p^n|b$. Show that this fails if $p$ is not prime.

14. (Section 2.5) Let $a, b, c$ be positive integers. Prove that $(a, \text{lcm}(b, c)) = \text{lcm}((a, b), (a, c))$, and that \(\text{lcm}(a, (b, c)) = \text{lcm}(\text{lcm}(a, b), \text{lcm}(a, c))\).

15. (Section 2.5) Show that for any $n \in \mathbb{Z}$, the numbers $6n - 1, 6n + 1, 6n + 2, 6n + 3$ and $6n + 5$ are pairwise relatively prime.

16. (Section 2.6) Solve the following linear Diophantine equation. Determine whether positive solutions exist, and if so how many.

$$63x - 37y = 3.$$ 

17. (Section 2.6) Find all $m$ such that $7x + 31y = m$ has exactly two positive solutions.
18. (Section 2.6) Find a number $n$ which when divided by 29 leaves a remainder of 4 and when divided by 31 leaves a remainder of 3. Solve this by converting this word problem into a linear diophantine equation in two variables.

19. (Section 3.1) True or false: $-2 \equiv 31 \pmod{11}$, $77 \equiv 5 \pmod{12}$.

20. (Section 3.1) Compute $2^{83} \pmod{7}$ (that is, find the least nonnegative element in its residue class).

21. (Section 3.1) For which positive integers $m$ does the congruence $75 \equiv 19 \pmod{m}$ hold?

22. (Section 3.1) Prove or disprove: $a \equiv b \pmod{m}$ implies $a^2 \equiv b^2 \pmod{m}$.

23. (Section 3.1) Suppose $m$ and $n$ are odd and not divisible by 3. Show that $24(n^2 - m^2)$.

24. (Section 3.1) Show that $3^{2n+5} + 2^{4n+1}$ is divisible by 7 for every $n \geq 1$.

25. (Section 3.1) Prove that if $a \equiv b \pmod{m}$ then $(a, m) = (b, m)$.

26. (Section 3.1) Prove or disprove: if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ and $c|a$ and $d|b$ then $\frac{a}{c} \equiv \frac{b}{d} \pmod{m}$.

27. (Section 3.2) Write down all elements in $U_{15}$ and $U_{32}$.

28. (Section 3.2) Find the inverse of 67 mod 119.

29. (Section 3.2) Solve $42x \equiv 90 \pmod{156}$; your answer(s) should be in $\mathbb{Z}/156\mathbb{Z}$.

30. (Section 3.3) Solve the system $x \equiv 7 \pmod{9}$, $x \equiv 0 \pmod{10}$, and $x \equiv 3 \pmod{7}$.

31. (Section 3.3) Determine if the following system has a solution, and if so, find it. $x \equiv 4 \pmod{6}$, $x \equiv 8 \pmod{12}$, $x \equiv 12 \pmod{18}$.

32. Prove that exponentiation is not associative, that is, $a^{(b^c)} \neq (a^b)^c$ for $a, b, c$ positive integers.

33. Similarly, prove that division is not associative, that is, $(a/b)/c \neq a/(b/c)$, for nonzero real numbers $a, b, c$.

34. (Section 4.1) Use Fermat’s little theorem to find the least nonnegative representative of $31^{100} \pmod{19}$. Same for $2^{1000} \pmod{31}$.

35. (Section 4.1) Use Fermat’s little theorem and the Chinese Remainder theorem to deduce that $n_{13} \equiv n \pmod{2730}$ for any $n \in \mathbb{N}$.

36. (Section 4.1) Show that if $p > 3$ is prime, then $ab^p - ba^p$ is divisible by $6p$. Hint: explain why it suffices to show that this expression is 0 mod each of 2, 3 and $p$. Then show these three congruences, using Fermat’s little theorem for $p$.

37. (Section 4.2) Determine $\phi(2730)$ and $\phi(1800)$.

38. (Section 4.2) Find all $n$ such that $\phi(n) = 12$. 
39. (Section 4.3) Use Euler’s theorem to find the least nonnegative representative of $3^{340} \pmod{341}$. Same for $7^{100} \pmod{100}$.

40. (Section 4.3) Prove that $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$ if $(m, n) = 1$.

41. (Section 4.3) Prove that $a^{560} \equiv 1 \pmod{561}$ for every $a$ such that $(a, 561) = 1$ but 561 is not prime. So 561 is called a Carmichael number.

42. (Section 4.4) Find all solutions to $x^4 \equiv 1 \pmod{13}$.

43. (Section 4.4) Suppose $p$ is prime. Show that if $a \not\equiv 1 \pmod{p}$ then $\sum_{i=0}^{p-1} a^i \equiv 1 \pmod{p}$.

44. (Section 7.1) Determine $\text{ord}_{42}(11)$, $\text{ord}_{54}(13)$ and $\text{ord}_{31}(5)$.

45. (Section 7.1) For which $m$ in the set $\{54, 79, 686, 752\}$ does there exist a primitive root mod $m$?

46. (Section 7.1) Find one primitive root mod 19 and use this to find all primitive roots mod 19.

47. (Section 7.1) (a) Suppose $g$ is a primitive root mod $mn$. Prove that it is a primitive root mod $m$. (b) Give an example of integers $g, m, n$ such that $g$ is a primitive root mod $m$ and mod $n$ but not a primitive root mod $mn$.

48. (Section 7.1) Suppose there is an integer $a$ such that $a^{\phi(n)/q}$ is not equivalent to 1 (mod $n$) for any prime divisor $q$ of $\phi(n)$. Show that $a$ is a primitive root mod $n$.

49. (Section 7.2) For which odd primes can we solve $x^2 \equiv -1 \pmod{p}$? Hint: consider two cases: $p \equiv 1 \pmod{4}$ and $p \equiv 3 \pmod{4}$; relate this question to the index.

50. (Section 7.2) Compute $\lambda(n)$ for $n \in \{800, 2268, 2730\}$.

51. (Section 7.2) What is the largest integer $m$ such that $a^{12} \equiv 1 \pmod{m}$ for all $a$ such that $(a, m) = 1$?

52. (Section 7.2) Suppose $g$ is a primitive root mod a prime $p$ and $p \equiv 1 \pmod{4}$. Show that $-g$ is also a primitive root mod $p$. Give an example to show that this fails if $p \equiv 3 \pmod{4}$.

53. (Section 7.3) Suppose $g$ and $h$ are primitive roots mod $n$. Show that

$$\log_h(y) \equiv \log_h(g) \log_g(y) \pmod{\phi(n)}$$

where $\log_a(b) = x$ iff $a^x \equiv b \pmod{n}$.