ELEMENTARY NUMBER THEORY

FINAL

(1) Complete the following definitions: for integers a, b, d, p we say that
   (a) $b \mid a$ if $a = bc$ for some $c \in \mathbb{Z}$.
   (b) a is a unit if $a \mid 1$.
   (c) p is irreducible if p is a nonunit, and if $p = ab$ implies that a or b is a unit.
   (d) p is prime if p is a nonunit, and if $p \mid ab$ implies that $p \mid a$ or $p \mid b$.
   (e) $d = \gcd(a, b)$ if $d \mid a$ and $d \mid b$, and if $e \mid a$ and $e \mid b$ implies $e \mid d$.

(2) Solve the following problems.
   (a) What is 40! mod 41?
   By Wilson, $40! \equiv -1 \bmod 41$.
   (b) What is 39! mod 41? BTW, if you can't remember whether it's $+1$ or -1, compute $(p-1)!$ mod p for some small primes.
   We have $40! \equiv -1 \equiv 40 \bmod 41$, hence $39! \equiv 1 \bmod 41$.
   (c) What is 38! mod 41?
   We have $38! \equiv \frac{1}{39} \equiv \frac{1}{-2} \equiv \frac{42}{-2} = -21 \equiv 20 \bmod 41$. Again, if you did not see this, you should have computed some small examples.

(3) Show that $\gcd(ab, a+b) = 1$ if $\gcd(a, b) = 1$.

Solution 1: Assume that there is a prime p with $p \mid \gcd(ab, a+b)$. Then $p \mid ab$, hence $p \mid a$ or $p \mid b$. But then $p \mid (a+b)$ shows that $p \mid a$ and $p \mid b$, hence $p \mid \gcd(a, b)$: contradiction.

Solution 2: $\gcd(ab, a+b) \mid \gcd(a, a+b)\gcd(b, a+b) = \gcd(a, b)\gcd(b, a) = 1$.

Solution 3: By Bezout we have $1 = ax + by$. Squaring yields

$$1 = a^2x^2 + 2abxy + b^2y^2 = 2abxy + (a+b)(ax^2 + by^2) - ab(x^2 + y^2)$$
$$= ab(2xy - x^2 - y^2) + (a+b)(ax^2 + by^2).$$

This shows that $\gcd(ab, a+b) \mid 1$.

(4) (a) Solve the congruence $17m \equiv 1 \bmod 100$.
   Euclid's algorithm gives $100 - 5\cdot 17 = 15$, $17 - 15 = 2$, $15 - 2\cdot 7 = 1$, hence $1 = 15 - 2\cdot 7 = 15 - 7(17-15) = 8\cdot 15 - 7\cdot 17 = 8(100 - 5\cdot 17) - 7\cdot 17 = 8\cdot 100 - 47\cdot 17$. This shows that $m \equiv -47 \equiv 53 \bmod 100$.
   You can also use the idea $\frac{1}{17} \equiv \frac{101}{17} \equiv \cdots \equiv \frac{901}{17} = 53 \bmod 100$.
   Finally, you may try your luck with the Chinese remainder theorem and solve $17m \equiv 1 \bmod 4$, $17m \equiv 1 \bmod 25$. Here $m \equiv 1 \bmod 4$ and $m \equiv 3 \bmod 25$ are easy to see, and even combining them into $m \equiv 53 \bmod 25$ can be done without even using pencil and paper.

(b) Solve $x^{17} \equiv 2 \bmod 101$.
A tricky question. The hint was that it was part b) of a problem.
From $x^{17} \equiv 2 \bmod 101$ we get $x^{17\cdot 53} \equiv 2^{53} \bmod 101$. Now $x^{17\cdot 53} = x^{1+9\cdot 100} \equiv x \bmod 101$, since $x^{100} \equiv 1 \bmod 101$ by Fermat. Thus $x \equiv 2^{53} \bmod 101$.
By the way, $2^{50} \equiv (\frac{2}{101}) = -1 \bmod 101$, hence $x \equiv -8 \bmod 101$.

(5) Is 17 a square mod 103? Justify your answer.

$(\frac{17}{103}) = (\frac{103}{17}) = (\frac{1}{17}) = +1$, and since 103 is prime, 17 is indeed a square mod 103.

(6) Solve the system of congruences

$$x \equiv 11 \bmod 17$$
$$x \equiv 17 \bmod 11.$$

We may replace the second congruence by $x \equiv 6 \bmod 11$. Euclid and Bezout tell us that $2 \cdot 17 - 3 \cdot 11 = 1$. Thus $x \equiv 6 \cdot 2 \cdot 17 - 11 \cdot 3 \cdot 11 \equiv 176 \equiv 28 \bmod 187$.

(7) Let q and $p = 4q + 1$ be primes. Show that $(\frac{2}{p}) = -1$.

If $q = 2$, then $p = 9$ is not prime. Thus q is odd, hence $p = 4q + 1 \equiv 5 \bmod 8$, and thereore $(\frac{2}{p}) = -1$ by the second supplementary law.

Extra credit: show that 2 is a primitive root mod p.
The order of 2 divides $p - 1 = 4q$, hence is one of 1, 2, 4, 2, q, $2q$, or $4q$. Since $2^{2q} \equiv -1 \bmod p$, the cases 1, 2, q and $2q$ cannot occur. Also, $2^4 \equiv 1 \bmod p$ would imply $p = 3$ or $p = 5$, which cannot occur. Thus the order must be $4q$, hence 2 is a primitive root mod p.

(8) Compute the class number $h(-47)$.

You will find the reduced forms $(1, 1, 12)$, $(2, \pm 1, 6)$ and $(3, \pm 1, 4)$. Thus $h(-47) = 5$.

(9) Reduce the form $(17, 21, 7)$.

$(17, 21, 7) \sim (7, -21, 17) \sim (7, 7, 3) \sim (3, -7, 7) \sim (3, -1, 3) \sim (3, 1, 3)$.

(10) Explain why $2 \cdot 13 = (4 + \sqrt{-10})(4 - \sqrt{-10})$ is an example of nonunique factorization.
The factors are irreducible and do not differ by units.