AC, December 2008

M3P14 Elementary Number Theory
Sheet 3: Solutions.

(1) We use the formula

$$\sigma(n) = \prod \frac{p_i^{r_i+1} - 1}{p_i - 1}$$

hence

$$\begin{aligned} \sigma(10) &= (1+2)(1+5) = 18 \\ \sigma(20) &= (1+2+4)(1+5) = 42 \\ \sigma(1728) &= \sigma(2^6 3^3) = (127)(40) = 5080 \end{aligned}$$

(3) Assume to the contrary that $5, p_2, ...p_r$ are all the primes $\equiv -1 \mod 6$; consider

$$N = 6p_2 \cdots p_r + 5 \equiv -1 \mod 6,$$

then none of the p_i can divide N; indeed 5 does not divice N and if $i \geq 2$ then $\text{hcf}(p_i, N)|5$ hence $\text{hcf}(p_i, N) = 1$. Look now at the prime factorization of N:

$$N = q_1 q_2 \cdots q_s \equiv -1 \mod 6$$

(possibly with repetitions); a prime other than 3 can only be $\equiv \pm 1 \mod 6$ (why?) and clearly 3 does not divide N (why?) hence $q_i \equiv \pm 1 \mod 6$; but then at least one of the $q_i \equiv -1 \mod 6$, a contradiction.

(5) We know that $(\mathbb{Z}/11\mathbb{Z})^\times \cong \mathbb{Z}/10\mathbb{Z}$ so we know that there are $\varphi(1) = 1$ element of order 1, $\varphi(2) = 1$ element of order 2, $\varphi(5) = 4$ elements of order 5 and $\varphi(10) = 4$ elements of order 10. Finally 2 is a primitive root $\mod 11$ and

the elements of order 10 are 2, $2^3 \equiv 8$, $2^7 \equiv 7$, $2^9 \equiv 6$;

the elements of order 5 are $2^2 \equiv 4$, $2^4 \equiv 5$ $2^6 \equiv 9$ $2^8 \equiv 3$;

the element of order 2 is $2^5 \equiv 10$.

(6) The first step is to make sense of the question: which is meant, multiplicative or additive order? It should be clear that multiplicative order is meant: Let $a \in \mathbb{Z}$ have order k in $(\mathbb{Z}/m\mathbb{Z})^\times$, etc. Next you should persuade yourself that the problem is *equivalent* to the following:

Problem. Prove that the *additive* order of $h \in \mathbb{Z}/k\mathbb{Z}$ is k if and only if $\text{hcf}(h, k) = 1$.

In turn, this is equivalent to saying that the following two statements are equivalent:

(a) For all m, k divides hm implies k divides m.

(b) $\text{hcf}(h, k) = 1$.

(It is easy to show that (a) and (b) are equivalent: do it!)

(8) Let p be prime; then $(\mathbb{Z}/p\mathbb{Z})^\times$ is a disjoint union of subsets $\{g, g^{-1}\}$; these are two-elements subsets except when $\{g, g^{-1}\} = \{-1\}$ and when $\{g, g^{-1}\} = \{1\}$. Taking the product of all elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ we get

$$\prod_{a=1}^{p-1} a \equiv 1 \times (-1) \times \prod gg^{-1} \equiv -1 \mod p$$

On the other hand, if n is composite, then $n = km$ for some $1 < k, m < n$, therefore $k|(n-1)!$ (for example) so $\mathrm{hcf}(n, (n-1)!) > 1$, that is, $(n-1)! \notin (\mathbb{Z}/n\mathbb{Z})^\times$.

(9) Here is a table of indices $\mod 17$ in the base 3; recall that the index function I takes an invertible integer $\mod p$ to an integer $\mod p-1$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$I(a)$	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

We solve

$$4x \equiv 11 \mod 17,$$

that is

$$I(4) + I(x) \equiv I(11) \mod 16.$$

We conclude

$$I(x) \equiv I(11) - I(4) \equiv 7 - 12 \equiv 11 \mod 16, \quad \text{that is,} \quad x \equiv 7 \mod 17.$$

Next we solve

$$5x^6 \equiv 7 \mod 17, \quad \text{that is,} \quad I(5) + 6I(x) \equiv I(7) \mod 16,$$
$$\text{and} \quad 6I(x) \equiv 6 \mod 16.$$

This gives $I(x) \equiv 1, 9 \mod 16$ and $x \equiv 3, 14 \mod 17$.

(10) (a) If $p - 1 = km$, then in $\mathbb{F}_p[X]$ (the "ring" of polynomials in the variable X with coefficients in the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$) we can factor

$$x^{p-1} - 1 = (x^k - 1)(1 + x^k + x^{2k} + \cdots + x^{k(m-1)});$$

we know that this polynomial has $p - 1 = km$ distinct roots in $\mathbb{F}_p$; it follows that the two polynomials on the right hand side each have the maximum allowed number of roots, k and $k(m-1)$ respectively.

(b) The equation is *equivalent* to the equation

$$kI(x) \equiv I(a) \mod p-1$$

therefore, from what we know, a solution exists if and only if $\mathrm{hcf}(k, p-1)$ divides $I(a)$ and, assuming that is the case, there are then $\mathrm{hcf}(k, p-1)$ solutions.

(c) Taking indices modulo 3 this is equivalent to

$$111I(x) \equiv 6 \mod 1986.$$

Now $\mathrm{hcf}(111, 1986) = 3$ divides 6, therefore there are 3 solutions.

(12) This follows a well-known procedure and it should not have been difficult for you to answer this question.

Assume for starts that $p \equiv 1 \mod 8$; this is the same as saying $p = 8m+1$ for some positive integer m, and $N = 4m$, and then we have the following table:

$-2j$	-2	-4	$\dots$	$-2(2m)$	$-2(2m+1)$	$\dots$	$-2(4m-1)$	$-2(4m)$
$(-2)_j$	-2	-4	$\dots$	$-4m$	$4m-1$	$\dots$	3	1

From this we can deduce: If $p = 8m+1$, then $\nu_p(-2) = 2m$ (we have just worked out from the definition a formula for $\nu_p(-2)$) and (from the Gauss lemma) $\left(\frac{-2}{p}\right) = 1$. The other cases ($p \equiv 3 \mod 8$, $p \equiv 5 \mod 8$, $p \equiv 7 \mod 8$) are similar and the details are left to you.