HW #6 Solutions

11.6 This translates into

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 2 \mod 7. \end{cases}$$

Solving $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 2 \mod 7 \end{cases}$ is super easy, as the answer must be

$$x \equiv 2 \mod 21.$$

So we are left with $\begin{cases} x \equiv 2 \mod 21 \\ x \equiv 3 \mod 5 \end{cases}$.

$x \equiv 2 \mod 21 \implies x = 2 + 21k$,

$2 + 21k \equiv 3 \mod 5 \implies k \equiv 1 \mod 5.$

So $x = 2 + 21(1 + 5m) = 2 + 21 + 105m$,

so $x = 23 + 105m$, or $x \equiv 23 \pmod{105}$.

11.9 We require $\gcd(m_i, m_j) = 1$ for each pair of moduli.
If this is true, then we can solve $\begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \\ x \equiv a_3 \ (m_3) \end{cases}$ by two applications of the ordinary Chinese Remainder Theorem.

By CRT, there is a solution $x \equiv b \ (m_1 m_2)$ to $\begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \end{cases}$ as $\gcd(m_1, m_2) = 1$. By CRT again, there is a solution $x \equiv c \ (m_1 m_2 m_3)$ to $\begin{cases} x \equiv b \ (m_1 m_2) \\ x \equiv a_3 \ (m_3) \end{cases}$, as $\gcd(m_1 m_2, m_3) = 1$.

One can clearly continue this argument inductively to any number of equations.

#3 $x^2 \equiv 1 \pmod{105}$

via

$$\begin{cases} x^2 \equiv 1 \bmod 3 \\ x^2 \equiv 1 \bmod 5 \\ x^2 \equiv 1 \bmod 7 \end{cases}$$

The solutions mod 3, 5, and 7 are very easy ~~to~~ to see.

They are
$$\begin{cases} x \equiv \pm 1 \bmod 3 \\ x \equiv \pm 1 \bmod 5 \\ x \equiv \pm 1 \bmod 7 \end{cases}$$

Then the idea is that for each combination of choices, we get a single solution mod 105.

for example:
$$\left.\begin{array}{l} x \equiv 1 \ (3) \\ x \equiv -1 \ (5) \\ x \equiv 1 \ (7) \end{array}\right\} \longleftrightarrow x \equiv 64 \bmod 105$$

In total, we have

$$\left.\begin{array}{l} x \equiv 1 \ (3) \\ x \equiv 1 \ (5) \\ x \equiv 1 \ (7) \end{array}\right\} \longleftrightarrow x \equiv 1 \ (105) \qquad \left.\begin{array}{l} x \equiv 1 \ (3) \\ x \equiv 1 \ (5) \\ x \equiv -1 \ (7) \end{array}\right\} \Longleftrightarrow x \equiv 76 \ (105)$$

$$\left.\begin{array}{l} x \equiv 1 \ (3) \\ x \equiv -1 \ (5) \\ x \equiv 1 \ (7) \end{array}\right\} \longleftrightarrow x \equiv 64 \ (105) \qquad \left.\begin{array}{l} x \equiv 1 (3) \\ x \equiv -1 (5) \\ x \equiv -1 \ (7) \end{array}\right\} \Longleftrightarrow x \equiv 34 \ (105)$$

$$\left.\begin{array}{l} x \equiv -1 \ (3) \\ x \equiv 1 \ (5) \\ x \equiv 1 \ (7) \end{array}\right\} \longleftrightarrow x \equiv 71 \ (105). \qquad \left.\begin{array}{l} x \equiv -1 \ (3) \\ x \equiv 1 \ (5) \\ x \equiv -1 \ (7) \end{array}\right\} \longleftrightarrow x \equiv 41 \ (105)$$

$$\left.\begin{array}{l} x \equiv -1 \ (3) \\ x \equiv -1 \ (5) \\ x \equiv 1 \ (7) \end{array}\right\} \longleftrightarrow x \equiv 29 \ (105) \qquad \left.\begin{array}{l} x \equiv -1 \ (3) \\ x \equiv -1 \ (5) \\ x \equiv -1 \ (7) \end{array}\right\} \longleftrightarrow x \equiv 104 \ (105)$$

So the solutions to $x^2 \equiv 1 \bmod 105$ are $x \equiv 1, 29, 34, 41, 64, 71, 76, 104 \pmod{105}$. ☒

$\boxed{12.1}$ $5 \longmapsto 5+1=6$, so after 1 step we get $2, 3, 5$

$2,3,5 \longmapsto 2\cdot3\cdot5+1 = 31$, so after 2 steps we get $2, 3, 5, 31$

$2,3,5,31 \longmapsto 2\cdot3\cdot5\cdot31+1 = 931$, which is $7^2 \cdot 19$.

So after 3 steps we get $2,3,5,7,19,31$

And now the numbers get too large. ∎

$\boxed{12.3}$ This is a great, but quite hard, question. I'll share my favorite way of showing $A_p \equiv 0 \bmod p$.

Group the summands like $\frac{1}{k} + \frac{1}{p-k} = \frac{p}{k(p-k)}$.
Each numerator is now divisible by p, so that adding the $\frac{p-1}{2}$ remaining fractions will also have numerator divisible by p. Very clever!

Part b is <u>very</u> hard to prove. ∎

$\boxed{13.1}$ How large is $F(x)$? It's clear that $F(x+5) = F(x)+1$, and $F(2)=1$. So $F(x)$ increases by 1 when x increases by 5. As x gets large, this means

$$\frac{F(x)}{x} \approx \frac{1}{5}.$$

[Stated more precisely, we see that $\frac{F(2+5x)}{x} \longrightarrow 1$].

For part (b), we have that $S(x) \approx \sqrt{x}$, & since $\frac{\sqrt{x}}{x} \longrightarrow 0$ as x gets large, we can say most numbers are not squares. ∎

$\boxed{13.3}$ For each k with $1 \le k \le n$, we have that $k \mid n!$

as $n! = 1 \cdot 2 \cdot \dots \cdot k \cdot (k+1) \cdot \dots \cdot n$.

So for k in $2, \dots, n$ we have that $k \mid n! + k$.

As $k < n! + k$, we see that $n! + k$ is not prime.

So the $(n-1)$ numbers $n!+2, \dots, n!+n$ are all composite. ∎

Aside: though these are $n-1$ composite numbers, we should sometimes expect there to be earlier strings of $n-1$ composite numbers. For instance, $3!+2, 3!+3 = 8, 9$, which is the 1st occurrence of consecutive composite numbers.

$4!+2, 4!+3, 4!+4 = 26, 27, 28$,

but the 1st occurrence of 3 consecutive composite numbers is $8, 9, 10$.

I have no idea what is known here, but I think it's a nice question to ask. //

$\boxed{13.5}$ By Prime Num. Theorem, $\pi(X) \approx \frac{X}{\log X}$. There are X integers up to X, so choosing one at random gives a chance $\approx \frac{X/\log X}{X} = \frac{(\text{prob success})}{(\text{total})} = \frac{1}{\log X}$.

If we assume these choices are independent, then choosing twice $\rightsquigarrow \left(\frac{1}{\log X}\right)^2$. So making X 2-choices $\rightsquigarrow \frac{X}{(\log X)^2}$.

Of course, it's not really independent, + the dependence or independence is the underlying hard question. ∎

#9 If $n!+1$ is prime, then we're done.
Otherwise, say $p \mid n!+1$. Write $n! = q_1^{a_1} \cdots q_k^{a_k}$,
and note that every prime less than n occurs in the factorization of $n!$

If $p = q$ for one of the primes $q \mid n!$, then we have $p \mid n!$, $p \mid n!+1$, & so $p \mid (n!+1) - n! = 1$.

But clearly $p \nmid 1$, & so $p \neq q$ for any q appearing in the factorization of $n!$
This method allows us to generate a prime larger than n for any n. ∎

14.3 The next is $\frac{3^7-1}{2} = 1093$.
For n even, write $n = 2k$. Then $\frac{3^{2k}-1}{2} = \frac{9^k-1}{2}$.
But $9 \equiv 1 \mod 8$, So $9^k - 1 \equiv 0 \ (8)$, & thus $4 \mid \frac{9^k-1}{2}$. ∎

Similarly, if n is a multiple of 5, write $n = 5k$.
Then $\frac{3^{5k}-1}{2} = \frac{243^m - 1}{2}$. Notice $243 - 1 = 2 \cdot 11^2$.

So $243^m - 1 \equiv (2 \cdot 11^2 + 1)^m - 1 \equiv 1^m - 1 \equiv 0 \mod 11^2$,
& so $\frac{243^m-1}{2}$ is divisible by 11^2. [And it's an integer as $243^m, 1$ both odd]. ∎
We don't know if there are infinitely many!

$\boxed{15.1}$ As $\gcd(m,n)=1$, if $a_1, a_2, \dots, a_k$ are the divisors of m and $b_1, b_2, \dots, b_\ell$ are the divisors of n, then there is no overlap between the a_i and b_j terms. So any divisor d of mn can be written uniquely as $d = ab$, where $a = \gcd(d,m)$, $b = \gcd(d,n)$.
Conversely, if $a|m$, $b|n$, then $ab|mn$.

So $\sigma(mn) = \sum a_i b_j = a_1b_1 + a_1b_2 + a_1b_3 + \cdots + a_k b_{\ell-1} + a_k b_\ell$

$$= (a_1 + a_2 + \cdots + a_k)(b_1 + b_2 + \cdots + b_\ell).$$

$$= \sigma(m)\sigma(n). \blacksquare$$

$\boxed{15.2}$ $\sigma(10) = \sigma(2)\sigma(5) = 3 \cdot 6 = 18$

$\sigma(20) = \sigma(4)\sigma(5) = 7 \cdot 6 = 42$

$\sigma(1728) = 5080$ $\blacksquare$

$\boxed{15.6}$ This is a great question!
The easily checked ones are 6, 8, 10, 14, 15, 21, 22, 26, 27, 33, 34, 35, 38, 39, 46.

A product perfect number is either a product of distinct primes pq, or p^3.
So $101 \cdot 103 = 10403$ is product perfect.
If m is divisible by distinct primes p, q, then $\frac{m}{p}, \frac{m}{q}$ are divisors, & so we want $m = (\text{product of divisors}) \geq \frac{m^2}{pq}$.
But then we need $m \cdot pq \geq m^2 \Longrightarrow m = pq$. Conversely, if these are the only factors, then it's clear m is product perfect.
If $m = p^k$, then divisors are $1, p, \dots, p^k$. For $1 \cdot p \cdot p^{k-1} = p^k$, then $k = 2$. $\blacksquare$