Math 235 (Fall 2009): Assignment 6 Solutions

1.1: Notice that $19808 = 1980 * 10 + 8$. Hence, by Fermat's little theorem, $2^{19808} \equiv (2^{10})^{1980} \cdot 2^8 \equiv 1^{1980} \cdot 2^8 \equiv (2^4)^2 \equiv (16)^2 \equiv 5^2 \equiv 25 \equiv 3 \pmod{11}$. Thus, $2^{19808} + 6 \equiv 9 \pmod{11}$. Using the Euclidean algorithm we can find $1 = 5 \cdot 9 + (-4) \cdot 11$. So, $5 \cdot 9 \equiv 1 \pmod{11}$. This means $(2^{19808} + 6)^{-1} \equiv 5 \pmod{11}$. Therefore, $(2^{19808} + 6)^{-1} + 1 \equiv 6 \pmod{11}$.

1.2: $12^2 \equiv 144 \equiv 28 \equiv -1 \pmod{29}$. Hence, $12^4 \equiv (-1)^2 \equiv 1 \pmod{29}$. Similarly $12^8 \equiv 12^{16} \equiv 1 \pmod{29}$.

By Fermat's little theorem, $12^{28} \equiv 1 \pmod{29}$. Thus, $12^{25} \cdot 12^3 \equiv 1 \pmod{29}$, i.e., $12^{25} \equiv 12^{-3} \equiv (12^3)^{-1} \pmod{29}$. Now notice that from $12^4 \equiv 1 \pmod{29}$, it follows that $12^{-3} \equiv 12 \pmod{29}$. So, $12^{25} \equiv 12 \pmod{29}$.

2.1: $x^4 - x^3 - x^2 + 1 = (x^3 - 1)(x - 1) + (-x^2 + x)$
$x^3 - 1 = (-x^2 + x)(-x - 1) + (x - 1)$
$-x^2 + x = (x - 1)(-x) + 0$

Hence, $gcd(x^4 - x^3 - x^2 + 1, x^3 - 1) = x - 1$ and
$x - 1 = (x^3 - 1) + (-x^2 + x)(x + 1)$
$= (x^3 - 1) + [(x^4 - x^3 - x^2 + 1) - (x^3 - 1)(x - 1)](x + 1)$
$= (x^3 - 1)(1 - (x - 1)(x + 1)) + (x^4 - x^3 - x^2 + 1)(x + 1)$
$= (x^3 - 1)(-x^2 + 2) + (x^4 - x^3 - x^2 + 1)(x + 1)$

2.2: $gcd = x^2 + x + 2$ and
$x^2 + x + 2 = (x^5 + x^4 + 2x^3 - x^2 - x - 2)(\frac{1}{4}x + \frac{1}{2}) + (x^4 + 2x^3 + 5x^2 + 4x + 4)(-\frac{1}{4}x^2 - \frac{1}{4}x + \frac{3}{4})$

2.3: $gcd = x^2 - \overline{1}$ and
$x^2 - \overline{1} = (x^4 + \overline{3}x^3 + \overline{2}x + \overline{4}) + (x^2 - \overline{1})(-x^2 - \overline{3}x)$

2.4: $gcd = \overline{4}x + \overline{6}$ and
$\overline{4}x + \overline{6} = (\overline{3}x^3 + \overline{5}x^2 + \overline{6}x)(\overline{2}x^2 + \overline{5}) + (\overline{4}x^4 + \overline{2}x^3 + \overline{3}x^2 + \overline{4}x + \overline{5})(\overline{2}x + \overline{4})$

2.5: $gcd = 3x - 3i$ (notice that this is the same as $gcd = x - i$) and
$3x - 3i = (x^2 + 1)(-x + i) + (x^3 - ix^2 + 4x - 4i)$

2.6: $gcd = \overline{1}$ and
$\overline{1} = (x^4 + x + \overline{1}) + (x^2 + x + \overline{1})(x^2 + x)$

3.1: Rephrasing the question: what are we using to conclude that $(g^a)^b = g^{ab} = (g^b)^a$?

By definition, $g^0 := 1$ and $g^{n+1} := g \cdot g^n$. Using this definition, one can see that in order to prove that $(g^a)^b = g^{ab}$ we need to use the associativity of the product in a ring.

3.2: If $p > 3$ and $g^3 = 1$, then $\{g, g^2, g^3, ..., g^{p-1}\} \neq \{\overline{0}, \overline{1}, ...\overline{p-1}\}$. In fact, $g^4 = g^3 g = g$, $g^5 = g^3 g^2 = g^2$ and so on. Hence, $\{g, g^2, g^3, ..., g^{p-1}\} = \{g, g^2\}$. A similar argument shows that $\{g, g^2, g^3, ..., g^{p-1}\} \neq \{\overline{0}, \overline{1}, ...\overline{p-1}\}$ if $g^2 = 1$.

Now, why isn't it desirable to have a g satisfying an equation like $g^n = 1$ for a small n? As we saw, in this case, $\{g, g^2, g^3, ..., g^{p-1}\}$ is a very small set. This makes the eavesdropper's task of finding g^{ab} given g^a and g^b much easier.

3.3: The elements are: $\overline{2}, \overline{6}, \overline{7}$ and $\overline{11}$.

3.4: Since the communication is assumed to be over an open channel, an eavesdropper could know g^a and g^b. Since he already know g, he can then know a and b. Therefore, he can compute g^{ab}, which was supposed to be a secret shared by A and B.

3.5: One possible way of doing this is the following:

A chooses a number a, B chooses b and C chooses c.

Similarly to what had been done before, B and C can share g^{bc}. They send this to A, which then computes $g^{abc} = (g^{bc})^a$.

A computes g^a and sends it to B and C. Now B computes $g^{ab} = (g^a)^b$ and sends it to C (which now can compute $g^{abc} = (g^{ab})^c$). C computes $g^{ac} = (g^a)^c$ and sends it to B (which can now compute $g^{abc} = (g^{ac})^b$).