PROGRAMMING AND DISCRETE MATHEMATICS (XX10190) SEMESTER 2 MATHEMATICS: PROBLEM SHEET 3 – SOLUTIONS

1. Calculate by hand:
$\mathrm{hcf}(261, 909)$; $x \in \mathbb{Z}$ such that $x = 12 \bmod 35$ and $x = -5 \bmod 47$; 3^{108} in $\mathbb{F}_{97}$; 13^{46} in $\mathbb{F}_{103}$; 18^{-1} in $\mathbb{F}_{73}^*$.
You do not need either a calculator (well, maybe, just) or much space. If you are writing down big numbers, in five figures or more, you are doing it the very slow way.
$909 = 3 \times 261 + 126$; $261 = 2 \times 126 + 9$; $126 = 14 \times 9$. *So* $\mathrm{hcf}(909, 261) = 9$. *(You could just spot the factor of* 9 *and stop there because you know that* 101 *is prime.)*
We had the next one on an earlier sheet. First, do Euclid with 35 *and* 47, *so* $47 = 35 + 12$ *and* $35 = 3 \times 12 - 1$ *so* $1 = 3 \times 12 - 35 = 3 \times (47 - 35) - 35 = 3 \times 47 - 4 \times 35$. *Now multiply up by* $12 - (-5) = 17$ *to get* $51 \times 47 - 68 \times 35 = 17$. *So* $x = 51 \times 47 - 5 = 68 \times 35 + 12$ *does the job, but rather than work that out I will take away* 47×35 *and use* $x = 21 \times 35 + 12 = 747$.
$3^{96} = 1$ *in* $\mathbb{F}_{97}$ *by Fermat, so* $3^{108} = 3^{12}$. *Let's be systematic:* $12 = 8 + 4$ *(*1100 *in binary) so* $3^2 = 9$, $3^4 = 9^2 = 81 = -16$, $3^8 = (-16)^2 = 256 = 62$. *Therefore* $3^{12} = 3^8 \times 3^4 = 62 \times -16$. *It's not hard to work that out directly, but I note that* $-16 = 81$ *and so* $62 \times -16 = 62 \times 81 = 186 \times 27 = -8 \times 27 = -216 = -22 = 75$.
Similarly, $46 = 32 + 8 + 4 + 2$ *(binary* 101110*) so in* $\mathbb{F}_{103}$ *we have* $13^2 = 169 = 66$, *then* $13^4 = 66^2 = 36 \times 121 = 36 \times 18 = 108 \times 6 = 5 \times 6 = 30$, *and* $13^8 = 30^2 = 900 = -27$, *and* $13^{16} = (-27)^2 = 9 \times 81 = 9 \times -22 = -198 = 8$, *and finally* $13^{32} = 64$. *Therefore* $13^{46} = 64 \times -27 \times 30 \times 66$, *which we could do directly: I would rather say that's* $-39 \times -27 \times 30 \times -37 = 1053 \times -1110 = 23 \times -80 = 23 \times 23 = 529 = 14$.
For the last one, simply notice that $4 \times 18 = 72 = -1$ *so* $18^{-1} = -4 = 69$.

2. Calculate the Legendre symbols

$$\left(\frac{81}{101}\right), \left(\frac{-81}{101}\right), \left(\frac{18}{103}\right), \left(\frac{91}{277}\right).$$

81 *is a square in* $\mathbb{Z}$ *so the first one is* 1 *and the second one is equal to* $\left(\frac{-1}{101}\right)$, *which is* 1 *because* $101 = 1$ *mod* 4 *(indeed* $-1 = 100$ *which is a square in* $\mathbb{Z}$*).*
For the third one we have $\left(\frac{18}{103}\right) = \left(\frac{9}{103}\right)\left(\frac{2}{103}\right) = \left(\frac{2}{103}\right)$ *(since* 9 *is a square in* $\mathbb{Z}$*) and* $\left(\frac{2}{103}\right) = 1$ *because* $103 = -1$ *mod* 8.
For the last one we have $\left(\frac{91}{277}\right) = \left(\frac{7}{277}\right)\left(\frac{13}{277}\right) = \left(\frac{277}{7}\right)\left(\frac{277}{13}\right)$, *because* $277 = 1$ *mod* 4, *by quadratic reciprocity. But* $277 = 4$ *mod* 13 *and* 4 *is a square, so* $\left(\frac{277}{13}\right) = 1$, *and* $277 = 4$ *mod* 7 *too. So* $\left(\frac{91}{277}\right) = 1$.

3. There are finite fields that are not $\mathbb{F}_p$: here is an example. In this question the constants are taken from the field $\mathbb{F}_3$.
Suppose that t satisfies $t^3 - t + 1 = 0$. Show that $t \notin \mathbb{F}_3$. Now let

$$\mathbb{F}_{27} = \{at^2 + bt + c \mid a,\, b,\, c \in \mathbb{F}_3\}.$$

Show that $\mathbb{F}_{27}$ has 27 elements. Show that it is a field, with the usual addition and multiplication: you need to check that multiplying two elements of $\mathbb{F}_{27}$ gives an element of $\mathbb{F}_{27}$ and that a non-zero element of $\mathbb{F}_{27}$ has an inverse.
Find a generator for the group $\mathbb{F}_{27}^*$.
$\mathbb{F}_{27}$ has 27 elements because $(a,b,c) \mapsto at^2 + bt + c$ is a bijection $\mathbb{F}_3^3 \to \mathbb{F}_{27}$. It's clearly onto: to show it's injective we need to check that $at^2 + bt + c = 0$ implies $a = b = c = 0$. So suppose $at^2 + bt + c = 0$: we may assume that $a = 1$, because if $a = 0$ then t satisfies a linear equation over $\mathbb{F}_3$, which can only be $0 = 0$ if $t \notin \mathbb{F}_3$. But now

$$x^3 - x + 1 = (x - b)(x^2 + bx + c) + l(x),$$

where $l(x)$ is linear. Putting $x = t$ we get $l(t) = 0$ so $l \equiv 0$ as before; but then putting $x = b$ we get $b^3 - b + 1 = 0$, which is not true for any $b \in \mathbb{F}_3$.
To check it's a field we need to show it's closed under multiplication and there are multiplicative inverses: everything else is obvious. Now

$$\begin{aligned}
&(at^2 + bt + c)(xt^2 + yt + z)\\
&\quad = axt^4 + (ay + bx)t^3 + (az + cx + by)t^2 + (bz + cy)t + cz\\
&\quad = axt(t-1) + (ay + bx)(t-1) + (az + cx + by)t^2 + (bz + cy)t + cz\\
&\quad = (ax + az + cx + by)t^2 + (-ax + ay + bx + bz + cy)t + (-ay - bx + cz)
\end{aligned}$$

so $\mathbb{F}_{27}$ is closed under multiplication.
The quickest method now is to jump to the last part. Notice that even though we don't yet know that $\mathbb{F}_{27}$ is a field, we do know that $t \in \mathbb{F}_{27}^*$, because its inverse is $1 - t^2$. Moreover, $t^2 \neq 0$ and

$$t^{13} = (t^3)^3 t^3 t = (t-1)^3 t^3 t = (t^3 - 1)t^3 t = (t+1)(t-1)t = t^3 - t = -1$$

so $t^{26} = 1$, so the order of t must be 26. Since $\mathbb{F}_{27}$ has 27 elements and one of them is zero, the order of $\mathbb{F}_{27}^*$ is at most 26, and since we've just found an element of order 26 it must be 26. So every non-zero element of $\mathbb{F}_{27}$ is invertible (i.e. $\mathbb{F}_{27}$ is indeed a field), and t is a generator for $\mathbb{F}_{27}^*$.

GKS, 21/3/17