PROGRAMMING AND DISCRETE MATHEMATICS (XX10190)
SEMESTER 2 MATHEMATICS: PROBLEM SHEET 1 – SOLUTIONS

1. Suppose that m and n are positive integers and $\mathrm{hcf}(m,n)=1$, and suppose that a and b are integers with $0\le a<m$, $0\le b<n$. How would you use Euclid's algorithm to find integers α and β such that $\alpha m+\beta n=a-b$? Hence explain how to find an integer N such that $N\equiv a \bmod m$ and $N\equiv b \bmod n$.
Euclid's algorithm finds λ and μ such that $\lambda m+\mu n=\mathrm{hcf}(m,n)=1$, so it is enough to take $\alpha=\lambda(a-b)$ and $\beta=\mu(a-b)$. Then take $N=\beta n+b=-\alpha m+a$.

2. Find a number N such that $N\equiv 94 \bmod 105$ and $N\equiv 13 \bmod 44$.
Doing it directly as above I got $\lambda=13$ and $\mu=-31$ (with $m=105$ and $n=44$), hence $\alpha=1053$ and $\beta=-2511$ and $N=-110471$. Adding $24\times 105\times 44$ to this gives the more sensible, but equally correct, answer of 409.

3. How many elements are there in $\mathbb{F}_p^*$? Deduce that if $a\in\mathbb{Z}$ and p is a prime, then $a^p\equiv a \bmod p$ (this is called Fermat's Little Theorem).
There are $p-1$. So if a is prime to p then we can think of a as being in $(\mathbb{Z}/p)^*=\mathbb{F}_p^*$, so $a^{p-1}=1$ because the order of the element divides the order of the group. Now multiply both sides by a. If $p|a$ then the equation just says $0=0$.

4. $561=3\times 11\times 17$. Calculate $\phi(561)$. Every prime that divides $\phi(561)$ also divides $560=2^4\times 5\times 7$, which is what $\phi(561)$ would be if 561 were prime. In fact $(\mathbb{Z}/561)^*$ has no element of order 32: deduce that $a^{560}\equiv 1 \bmod 561$ for every $a\in\mathbb{Z}$ coprime to 561 even though 561 is not prime.
$\phi(561)=561\times\frac{2}{3}\times\frac{10}{11}\times\frac{16}{17}=320$. But $320=64\times 5$. Since there is no element of $(\mathbb{Z}/561)^*$ of order 32, every element is of order dividing 16×5 and therefore dividing 560. So $a^{560}=1$ in $(\mathbb{Z}/561)^*$.

GKS, 7/3/17