## Linear Systems of Congruences

To solve a linear system of conguences, use the elimination method to get rid of one of the variables. The allowed mathematical operations are addition, subtraction, and multiplication (only by numbers relatively prime to the modulus). Remember if the modulus is $n$, then the only numbers that are allowed in the equations are 0,1,...,$n-1$. For example, if we want to solve the system

$x + y \equiv 1 \pmod 4$,

$x + 3y \equiv 1 \pmod 4$,

then you can choose to get rid of $y$. There are many ways in which you can do that. One of them is simply by adding the two equations up. Because when you do so, you'll get $4y$ in the result which is congruent to $0.y$, which is 0. So, this will enable you to get rid of $y$. Thus, by adding the two equations, you get $2x \equiv 2 \bmod 4$. Now solve this equation by the method we described in class to get: $x \equiv 1$ and $x \equiv 3$. When $x \equiv 1$, the first equation becomes: $1 + y \equiv 1$. Thus, $y \equiv 0$. Therefore, one solution of the above system is $x \equiv 1 \pmod 4$, $y \equiv 0 \pmod 4$. Now when $x \equiv 3$, the first equation becomes: $3 + y \equiv 1$. Thus, $y \equiv 2$. Therefore, another solution of the above system is $x \equiv 3 \pmod 4$, $y \equiv 2 \pmod 4$. **You are highly encouraged to check the "solutions?" which you got, because if you multiply by numbers that are not relatively prime to the modulus, then you may end up with values that you believe are solutions but they are not. This is likely, so be careful!.**

You can solve the system by choosing to get rid of $x$. You can do that in many ways. For example, you can subtract the first equation from the second to get $2y \equiv 0$. This equation has two solutions, namely $y \equiv 0$ and $y \equiv 2$ (you can find them by the same method we discussed Friday). Now you need to find $x$. This is the way to do it. When $y \equiv 0$, the first equation becomes $x \equiv 1$. Thus, $x \equiv 1 \pmod 4$, $y \equiv 0 \pmod 4$ is a solution. Now when $y \equiv 2$, the first equation becomes $x + 2 \equiv 1$. Thus, $x \equiv 3$. Therefore, $x \equiv 3 \pmod 4$, $y \equiv 2 \pmod 4$ is a second solution of the above system.

*Remark:*

**You are highly encouraged to check the "solutions?" which you got, because if you multiply by numbers that are not relatively prime to the modulus, then you may end up with values that you believe are solutions but they are not. This is likely, so be careful!.**

*Remark:*

**In one of the examples today, I wanted to find the multiplicative inverse of 93 (mod 119). If you remember, I wrote 1=(-25)(119)+(32)(93). Some people asked: how did u get that? Ok, gcd(93,119)=1. So, 1 can be written as a linear combination of 93 and 119. How to do that? The answer is by the algorithm we explained Friday. (See Friday's lecture.)**