Math 115. More Complicated Congruences

This handout discusses congruences in more than one variable. It roughly follows what we've done in class with congruences in one variable.

Definition. The notation $\mathbb{Z}[x_1,\dots,x_n]$ means the set of all polynomials in variables $x_1,\dots,x_n$ with integer coefficients.

In the following we'll consider only a congruence $f(x,y)\equiv 0 \pmod{m}$ with $f\in\mathbb{Z}[x,y]$ and $m\in\mathbb{Z}_{>0}$. Congruences in more than two variables are handled similarly.

Throughout this handout, $f\in\mathbb{Z}[x,y]$ and $m\in\mathbb{Z}_{>0}$.

Definition. Let $f,g\in\mathbb{Z}[x,y]$. We say that $f\equiv g\pmod{m}$ if all coefficients of $f-g$ are multiples of m. This holds if and only if $f-g=mh$ for some $h\in\mathbb{Z}[x,y]$. This is an equivalence relation on $\mathbb{Z}[x,y]$.

If $f\equiv g\pmod{m}$, then $f(a,b)\equiv g(a,b)\pmod{m}$ for all $a,b\in\mathbb{Z}$, so the congruences $f(x,y)\equiv 0\pmod{m}$ and $g(x,y)\equiv 0\pmod{m}$ have the same solutions.

Also, if $a_1\equiv a_2\pmod{m}$ and $b_1\equiv b_2\pmod{m}$, then $f(a_1,b_1)\equiv f(a_2,b_2)\pmod{m}$, so one can describe solutions of the congruence $f(x,y)\equiv 0\pmod{m}$ by giving a subset of $\mathscr{C}\times\mathscr{C}$, where $\mathscr{C}$ is a complete residue system modulo m.

Definition. The **number of solutions** of a congruence $f(x,y)\equiv 0\pmod{m}$ is the number of elements of the set $\{(r,s)\in\mathscr{C}\times\mathscr{C}: f(r,s)\equiv 0\pmod{m}\}$, where $\mathscr{C}$ is a complete residue system modulo m. This number is independent of the choice of $\mathscr{C}$.

One can define an equivalence relation $\equiv_m$ on $\mathbb{Z}\times\mathbb{Z}$ by saying that $(a,b)\equiv_m(a',b')$, or equivalently $(a,b)\equiv(a',b')\pmod{m}$, if $a\equiv a'\pmod{m}$ and $b\equiv b'\pmod{m}$. Then the set $\{(a,b)\in\mathbb{Z}\times\mathbb{Z}: f(a,b)\equiv 0\pmod{m}\}$ is a union of equivalence classes under this equivalence relation, and the number of solutions of $f(x,y)\equiv 0\pmod{m}$ (as defined above) is the number of these equivalence classes.

We won't define the degree of a congruence $f(x,y)\equiv 0\pmod{m}$. That can be defined using the same principles as one would use to define the degree of a polynomial in two (or more) variables. In other words, you first need to say what the degree of a monomial x^iy^j is (usually it's $i+j$).

Now we consider the Chinese Remainder Theorem. The statements we proved about how the Chinese Remainder Theorem applies to solutions of congruences in one variable can also be proved for congruences in two (or more) variables.

To begin, let $m_1,\dots,m_t$ be positive integers, pairwise relatively prime, and let $m=m_1\cdots m_t$. Let $\mathscr{C}$ and $\mathscr{C}_1,\dots,\mathscr{C}_t$ be complete residue systems modulo m and modulo $m_1,\dots,m_t$, respectively. Recall that we defined a function

$$\psi\colon\mathscr{C}\to\mathscr{C}_1\times\cdots\times\mathscr{C}_t\ ,$$

and showed that it is bijective. Recall also that ψ was defined by $\psi(r)=(r_1,\dots,r_t)$ for all $r\in\mathscr{C}$, where $r_i\in\mathscr{C}_i$ and $r_i\equiv r\pmod{m_i}$ for all i.

To deal with congruences in two variables, we define a similar function

$$\psi_2\colon \mathscr{C}\times\mathscr{C}\to(\mathscr{C}_1\times\mathscr{C}_1)\times\cdots\times(\mathscr{C}_t\times\mathscr{C}_t)\;,$$

by letting $\psi_2(r,s)=((r_1,s_1),\dots,(r_t,s_t))$ for all $r,s\in\mathscr{C}$, where $r_i,s_i\in\mathscr{C}_i$, $r_i\equiv r \pmod{m_i}$, and $s_i\equiv s \pmod{m_i}$ for all i.

The function ψ_2 is also bijective. Indeed, since its domain and codomain are finite sets with the same number m^2 of elements, it suffices to show that it is injective. This can be done by the same method as was done for ψ. Indeed, assume that $\psi_2(r,s)=\psi_2(r',s')$, with $r,s,r',s'\in\mathscr{C}$. Let r_i,s_i for all i be as in the definition of $\psi_2(r,s)$, and let r'_i,s'_i for all i be defined similarly for $\psi_2(r',s')$. If $\psi_2(r,s)=\psi_2(r',s')$, then $r_i=r'_i$ and $s_i=s'_i$ for all i; therefore $\psi(r)=(r_1,\dots,r_t)=(r'_1,\dots,r'_t)=\psi(r')$, which implies $r=r'$ since ψ is injective. Similarly $s=s'$, so $(r,s)=(r',s')$ and thus ψ_2 is injective.

Corresponding to a corollary from class on 24 September, we then have:

Corollary. *Let $m_1,\dots,m_t$, m, $\mathscr{C}$, and $\mathscr{C}_1,\dots,\mathscr{C}_t$ be as above, and let $f\in\mathbb{Z}[x,y]$. Let $\mathscr{C}'\subseteq\mathscr{C}\times\mathscr{C}$ be the set $\{(r,s)\in\mathscr{C}\times\mathscr{C} : f(r,s)\equiv 0 \pmod{m}\}$, and let $\mathscr{C}'_i\subseteq\mathscr{C}_i\times\mathscr{C}_i$ be similarly defined for all i. Then*

$$\psi_2(\mathscr{C}')=\mathscr{C}'_1\times\cdots\times\mathscr{C}'_t\;.$$

Proof. Let $r,s\in\mathscr{C}$, and let $((r_1,s_1),\dots,(r_t,s_t))=\psi_2(r,s)$. Then

$$\begin{aligned} f(r,s)\equiv 0 \pmod{m} &\iff f(r,s)\equiv 0 \pmod{m_i}\;\forall\, i \iff f(r_i,s_i)\equiv 0 \pmod{m_i}\;\forall\, i\\ &\iff (r_i,s_i)\in\mathscr{C}'_i\;\forall\, i \iff \psi_2(r,s)\in\mathscr{C}'_1\times\cdots\times\mathscr{C}'_t \end{aligned}$$

for the same reasons as in the earlier one-variable case. □

As a consequence, the number of solutions of the congruence $f(x,y)\equiv 0$ (mod m) is the product of the number of solutions (mod m_i) for all i, (as defined above), by the same proof as in the one-variable case.

As an example, we give another proof that, if $m_1,m_2\in\mathbb{Z}_{>0}$ are relatively prime, then $\phi(m_1m_2)=\phi(m_1)\phi(m_2)$, where ϕ is Euler's totient function. Indeed, for all $m>0$, $\phi(m)$ is the number of solutions of the congruence $xy\equiv 1 \pmod{m}$ (the proof is left to you as an exercise). Therefore we obtain the proof as an immediate consequence of the above corollary.

Finally, all of the above can also be done for systems of congruences (in the same modulus). Indeed, let f, $\mathscr{C}'$, and $\mathscr{C}'_1,\dots,\mathscr{C}'_t$ be as above. Let $g\in\mathbb{Z}[x,y]$ be another polynomial, and let $\mathscr{C}''$ and $\mathscr{C}''_1,\dots,\mathscr{C}''_t$ be defined similarly to $\mathscr{C}'$, etc., for the congruence $g(x,y)\equiv 0 \pmod{m}$ and mod m_i, respectively. Then $\mathscr{C}'\cap\mathscr{C}''$ represents the set of congruence classes of solutions of the system $f(x,y)\equiv g(x,y)\equiv 0 \pmod{m}$, and similarly $\mathscr{C}'_i\cap\mathscr{C}''_i$ represents solutions of the same congruences mod m_i for all i. Therefore

$$\begin{aligned} \psi_2(\mathscr{C}'\cap\mathscr{C}'')=\psi_2(\mathscr{C}')\cap\psi_2(\mathscr{C}'') &= (\mathscr{C}'_1\times\cdots\times\mathscr{C}'_t)\cap(\mathscr{C}''_1\times\cdots\times\mathscr{C}''_t)\\ &= (\mathscr{C}'_1\cap\mathscr{C}''_1)\times\cdots\times(\mathscr{C}'_t\cap\mathscr{C}''_t)\;. \end{aligned}$$