Computer Science Department - Rutgers University **Spring 2018**

CS 205: Diophantine Equations 16:198:205

In a variety of contexts, we may be interested in solving a system of equations with the additional restriction that *the values of the variables are restricted to be integers.* Consider as an example, the problem of finding integer solutions x, y to the following equation:

$$7x + 23y = 10. \tag{1}$$

In the usual approach, we might take the solution $x = (10 - 23y)/7$, but this does not guarantee that x will be an integer unless $10 - 23y$ is divisible by 7. The restriction to integer solutions adds an interesting wrinkle to the problem.

But consider the following approach - we can essentially reduce the problem by looking at arithmetic modulus some base. For any given value N, if the two sides are equal, we must also have

$$(7x + 23y) \equiv 10 \mod N. \tag{2}$$

Various choices of N can lead us to different observations. Consider, for instance, taking $N = 2$. In this case, since $7 \equiv 1 \mod 2$ and $23 \equiv 1 \mod 2$, it can be shown that

$$(7x + 23y) \equiv 1x + 1y \equiv x + y \equiv 0 \mod 2. \tag{3}$$

This tells us that for any integer solution (x, y), $x + y$ must be congruent to $0 \mod 2$, i.e., $x + y$ must be even. This is information we didn't have before, but it isn't necessarily the most informative. We know that either x and y are both even, or x and y are both odd.

Can we find an N that gives us more information? Consider $N = 7$. In this case, we have

$$(7x + 23y) \equiv 0x + 2y \equiv 2y \equiv 3 \mod 7. \tag{4}$$

We've reduced the original equation down to a single linear congruence in one variable: $2y \equiv 3 \mod 7$. What does this say about y? As in the proof of Fermat's Little Theorem, we can make use of the idea of the function $2n \mod 7$ as a bijective map from the numbers $S = \{0, 1, 2, 3, 4, 5, 6\}$ to itself. Because it is a bijection, it has an inverse and a moment or two of thought will suggest that the 'inverse' value of this function for 3 is 5. That is, $3 \equiv 2 * 5 \mod 7$. By the uniqueness of the inverse, the conclusion we must draw from this is that for any integer solution (x, y) to the original equation, we must have

$$y \equiv 5 \mod 7. \tag{5}$$

This tells us something very specific about just y alone - y must yield a remainder of 5 when divided by 7, or for some value of k in the integers, we have

$$y = 5 + 7k. \tag{6}$$

We can take a similar approach for the x term: taking $N = 23$, we have that

$$(7x + 23y) \equiv 7x + 0y \equiv 7x \equiv 10 \mod 23. \tag{7}$$

Left with the relation that $7x \equiv 10 \mod 23$, what can we say about x? Again we can argue that the map $7n \mod 23$ is a bijective map from the set $\{0, 1, 2, \ldots, 22\}$ to itself, hence 10 has some unique inverse under this map. But how can we find it? Note at this point that we have, via Fermat's Little Theorem, that

$$7^{23-1} \equiv 1 \mod 23. \tag{8}$$

Massaging this a little, we can write it in the following way:

$$10 * 7 * 7^{21} \equiv 10 * 1 \mod 23, \tag{9}$$

or

$$7 * (10 * 7^{21}) \equiv 10 \mod 23. \tag{10}$$

. Comparing this with the original congruence we are interested in, we see that

$$x \equiv 10 * 7^{21} \mod 23 \tag{11}$$

will satisfy the congruence $7x \equiv 10 \mod 23$. But what does this say about x? We can either compute it directly and take the remainder when divided by 23, or do some kind of computational simplification or expansion like the following (so as to be able to do it with pencil and paper if needed):

$$\begin{aligned} x &\equiv 10 * 7^{20} * 7 \\ &\equiv 10 * 49^{10} * 7 \\ &\equiv 10 * 3^{10} * 7 \\ &\equiv 10 * 3^{9} * 3 * 7 \\ &\equiv 30 * 27^{3} * 7 \\ &\equiv 7 * 4^{3} * 7 \\ &\equiv 49 * 4^{3} \\ &\equiv 3 * 4^{3} \\ &\equiv 12 * 16 \\ &\equiv 24 * 8 \\ &\equiv 1 * 8 \\ &\equiv 8 \mod 23 \end{aligned} \tag{12}$$

Hence we've arrived at $x \equiv 8 \mod 23$, which checks out, as $7 * 8 = 10 + 2 * 23$. At this point, we have arrived at the following conclusion: For any integer solution (x, y) to the original equation, we must have

$$\begin{aligned} y &\equiv 5 \mod 7 \\ x &\equiv 8 \mod 23. \end{aligned} \tag{13}$$

We can also think of this as specifying the 'form' of x and y relative to the given bases - in particular, for some integers k, m, we have that

$$\begin{aligned} y &= 5 + 7k \\ x &= 8 + 23m. \end{aligned} \tag{14}$$

But we have arrived here by effectively decoupling the two variables - we started with a relationship between both variables together, and reduced it to relationships involving a single variable at a time. What values of k and m are allowed? At this point, we can return to the original equation to re-couple to two variables:

$$\begin{aligned} 10 &= 7x + 23y \\ &= 7(8 + 23m) + 23(5 + 7k) \\ &= 56 + 161m + 115 + 161k \\ &= 171 + 161(m + k), \end{aligned} \tag{15}$$

or, simplifying:

$$m + k = -1. \tag{16}$$

That is, for x and y of those forms, any choice of m, k where $m+k = -1$ will suffice. Taking for instance $k = -1-m$, we have:

$$\begin{aligned} y &= 5 + 7(-1 - m) \\ x &= 8 + 23m, \end{aligned} \tag{17}$$

or

For any integer m, the values

$$\begin{aligned} y &= -2 - 7m \\ x &= 8 + 23m, \end{aligned} \tag{18}$$

are integer solutions to the equation $7x + 23y = 10$. Further, it can be argued that *any* solution must be of this form, by the uniqueness of the inverses used to solve the linear congruences.

Taking, as an example, $m = 0$, we get $x = 8$, $y = -2$, and $7 * 8 - 2 * 23 = 56 - 46 = 10$, verifying this as a solution.

Generalizing

Let P, Q be prime numbers, and M some integer. We want to derive integer solutions to the equation

$$Px + Qy = M. \tag{19}$$

From this, we can decouple the original equation into two congruences:

$$\begin{aligned} Px &\equiv M \mod Q \\ Qy &\equiv M \mod P \end{aligned} \tag{20}$$

We have, by Fermat's Little Theorem that

$$\begin{aligned} P^{Q-1} &\equiv 1 \mod Q \\ Q^{P-1} &\equiv 1 \mod P, \end{aligned} \tag{21}$$

and hence that

$$\begin{aligned} M * P * P^{Q-2} &\equiv M * 1 \mod Q \\ M * Q * Q^{P-2} &\equiv M * 1 \mod P, \end{aligned} \tag{22}$$

or

$$\begin{aligned} P[M * P^{Q-2}] &\equiv M \mod Q \\ Q[M * Q^{P-2}] &\equiv M \mod P. \end{aligned} \tag{23}$$

We get from this, and the uniqueness of inverses (mod Q, P) that we must have

$$\begin{aligned} x &\equiv M * P^{Q-2} \mod Q \\ y &\equiv M * Q^{P-2} \mod P. \end{aligned} \tag{24}$$

Note, with actual values for P, Q, M, we could reduce the above by calculating the actual remainders when divided by P, Q. But nevertheless the congruences must hold. We get then that for some integers k, m, we have

$$\begin{aligned} x &= M * P^{Q-2} + kQ \\ y &= M * Q^{P-2} + mP. \end{aligned} \tag{25}$$

However again, we have decoupled the variables from their original relationship. Substituting back in, we can derive a relationship between k and m:

$$\begin{aligned} M &= Px + Qy \\ &= P(M * P^{Q-2} + kQ) + Q(M * Q^{P-2} + mP) \\ &= M * P^{Q-1} + PQk + M * Q^{P-1}PQm \\ &= M[P^{Q-1} + Q^{P-1}] + PQ[k + m]. \end{aligned} \tag{26}$$

We can then solve this effectively to get a simple relationship between k and m, namely

$$k + m = M\left(\frac{1 - [P^{Q-1} + Q^{P-1}]}{PQ}\right). \tag{27}$$

The above is interesting, because while we know that k and m must be integers (and therefore their sum must be an integer), how can we be certain that for any given value of P or Q, the fraction above divides cleanly? The picture becomes a little more clear noting the following algebraic relationship:

$$1 - (P^{Q-1} + Q^{P-1}) = (P^{Q-1} - 1)(Q^{P-1} - 1) - P^{Q-1}Q^{P-1}. \tag{28}$$

Noting that in the above, $Q^{P-1} - 1$ must be divisible by P (why?) and that $P^{Q-1} - 1$ must be divisible by Q (why?), we get that $1 - (P^{Q-1} + Q^{P-1})$ must be divisible by PQ. Hence, the formula for $k + m$ above yields an integer. Solving for m in terms of k, and plugging in to the above formulas for x and y, we get that

For P, Q prime and integer M, any integer solutions x, y to

$$Px + Qy = M \tag{29}$$

must satisfy for some integer k,

$$\begin{aligned} x &= M * P^{Q-2} + kQ \\ y &= -M * \left(\frac{P^{Q-1} - 1}{Q}\right) - Pk. \end{aligned} \tag{30}$$

Again, it is worth noting that $P^{Q-1} - 1$ must be divisible by Q.

This gives us a nice explicit parameterization of integer solutions in terms of an integer parameter m. Note, the values above may be quite large (depending on P, Q) but can be potentially reduced by computing the mods explicitly in Eq. (24).

Generalizing Further Still

One way of synthesizing the above is the following:

For any prime P, the congruence

$$Ax \equiv D \mod P \tag{31}$$

is uniquely solved by

$$x \equiv DA^{P-2} \mod P. \tag{32}$$

If $A \not\equiv 0 \mod P$, then this solution is unique.

This utilizes Fermat's Little Theorem to generate the multiplicative inverse of $A \mod P$, multiplying it by D to generate the modular equivalent of D/A. Above, this generated the initial congruences for x and y, and by plugging these into the original equation again, we were able to solve for the full integer solutions. The thing that stops the previous solution from generalizing completely to equations like

$$Ax + By = C \tag{33}$$

is the possibility that A, B are not primes, and hence Fermat's Little Theorem does not hold (directly). Hence, it is worth considering congruences of the form

$$Ax \equiv 1 \mod N \tag{34}$$

for non-prime bases N. If this can be solved for x, we can generate solutions to the more general form needed to engineer solutions as above.

For any integers A, N, let x_0 be a solution to

$$Ax_0 \equiv 1 \mod N \tag{35}$$

if such a solution exists. In that case, the congruence

$$Ax \equiv D \mod N \tag{36}$$

is uniquely solved by

$$x \equiv Dx_0 \mod N. \tag{37}$$

Some experimentation will very quickly reveal that not all congruences of this form are solvable at all.

$$2x \equiv 1 \mod 4 \tag{38}$$

has no solutions, since if x is even, i.e., $x = 2k$, then $2x = 4k \equiv 0 \mod 4$, and if x is odd, i.e., $x = 2k + 1$, then $2x = 4k + 2 \equiv 2 \mod 4$. Hence there is no way to get a modulus of 1 in this instance.

But some are solvable:

$$5x \equiv 1 \mod 6 \tag{39}$$

has a relatively immediate solution of $x \equiv 5 \mod 6$, since $5 * 5 = 25 = 1 + 4 * 6$. So what differentiates the two cases? It is worth unpacking this into the 'form' notion of modular congruences. In the two cases above, we are asserting that there are integers k and m such that

$$\begin{aligned} 2x - 4k &= 1 \\ 5x - 6m &= 1. \end{aligned} \tag{40}$$

In the first case, it quickly becomes clear where the problem is: we can factor out a 2 yielding the equation $2(x-2k) = 1$. Since $x - 2k$ must be an integer, this implies that 2 evenly divides 1, which it does not. There are no integer solutions x, k that could possibly satisfy this equation. This generalizes immediately: if there is any shared (non-trivial) factor between A and N, then the equation $Ax - Nk = 1$ can have no integer solutions for x, k.

> If $\text{GCD}(A, N) \neq 1$, then $Ax \equiv 1 \mod N$ has no integer solutions.

In this second case, a quick eyeballing reveals a solution at $x = -1, m = -1$, which corresponds to the solution above, since $-1 \equiv 5 \mod 6$. In this case, we have that $\text{GCD}(5, 6) = 1$, in which case the above result does not apply. Can anything be concluded in this case, generally? Yes.

> If $\text{GCD}(A, N) = 1$, then $Ax \equiv 1 \mod N$ has integer solutions.

Consider the equation $5x - 6m = 1$. Previously, we would knock out the m-variable term by taking mods with respect to 6 to cancel that term. But in this case, that leads back to the problem we are trying to solve. So consider taking mods relative to a divisor of 6. In particular, we have

$$\begin{aligned} 1 &\equiv (5x - 6m) \mod 2 \\ &\equiv 1 * x - 0 * m \mod 2 \\ &\equiv x \mod 2. \end{aligned} \tag{41}$$

Hence any such x must satisfy $x \equiv 1 \mod 2$, i.e., x must be odd. Additionally, we have

$$\begin{aligned} 1 &\equiv (5x - 6m) \mod 3 \\ &\equiv 2 * x - 0 * m \mod 3 \\ &\equiv 2x \mod 3. \end{aligned} \tag{42}$$

And we can use the previous solution to solve this via $x \equiv 2^{3-2} \equiv 2 \mod 3$. Hence, we have the following decomposition based on the factorization $6 = 2 * 3$:

$$\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv 2 \mod 3. \end{aligned} \tag{43}$$

We can recombine these into a solution for x, noting that if $x = 2 + 3k$ for some k, then $x \equiv 0 + 1k \equiv 1 \mod 2$, or $k = 2j + 1$ for some j. Hence, we have

$$x = 2 + 3(2j + 1) = 5 + 6j, \tag{44}$$

or

$$5x \equiv 1 \mod 6 \implies x \equiv 5 \mod 6, \tag{45}$$

precisely the result found by inspection.

But how can we generalize this? Let $\textbf{inv}(A, N)$ be the multiplicative inverse of $A \mod N$, i.e., if it exists,

$$A * \textbf{inv}(A, N) \equiv 1 \mod N. \tag{46}$$

In the case that it exists, what can be said about it? Unpacking the above congruence, we have effectively that for some integer k,

$$A * \textbf{inv}(A, N) + N * k = 1. \tag{47}$$

Our standard trick at this point is to reduce the equation by taking mods with respect to one of the coefficients. In this case, modding with respect to N recovers the original congruence we wish to solve. The alternative then is to mod with respect to A, i.e.

$$\begin{aligned} 1 &\equiv (A * \mathbf{inv}(A, N) + N * k) \mod A \\ &\equiv N * k \mod A \\ &\equiv (N \mod A) * k \mod A, \end{aligned} \tag{48}$$

where $N \mod A$ is taken to be the remainder when N is divided by A. We get from the above that k must be congruent to $\mathbf{inv}(N \mod A, A)$. Taking k to be of the form

$$k = \mathbf{inv}(N \mod A, A) + Aj, \tag{49}$$

we recover from this that

$$\begin{aligned} 1 &= A * \mathbf{inv}(A, N) + N * k \\ &= A * \mathbf{inv}(A, N) + N * (\mathbf{inv}(N \mod A, A) + Aj), \end{aligned} \tag{50}$$

or

$$\mathbf{inv}(A, N) = \frac{1 - N * (\mathbf{inv}(N \mod A, A) + Aj)}{A} = \frac{1 - N * \mathbf{inv}(N \mod A, A)}{A} - Nj \tag{51}$$

Note, in the above, $(1 - N * \mathbf{inv}(N \mod A))$ must be divisible by A since

$$N * \mathbf{inv}(N \mod A, A) \equiv N * \mathbf{inv}(N, A) \equiv 1 \mod A. \tag{52}$$

The above yields the following recursive relationship for the inverse function:

$$\mathbf{inv}(A, N) \equiv \frac{1 - N * \mathbf{inv}(N \mod A, A)}{A} \mod N. \tag{53}$$

Since $N \mod A$ must satisfy $0 < N \mod A < A$, this in some sense represents a reduction of the original problem to a 'strictly smaller' problem - going from parameters (A, N) to parameters $(N \mod A, A)$. In this way, we may repeatedly reduce the problem to one more easily solved. A base case to work from here is the simple case that if $A = 1$, then $Ax \equiv 1 \mod N$ is solved by $x = 1$, i.e,

$$\mathbf{inv}(1, N) \equiv 1 \mod N. \tag{54}$$

Applying this to the previous example of $5x \equiv 1 \mod 6$, we have

$$\begin{aligned} \mathbf{inv}(5, 6) &\equiv \frac{1 - 6 * \mathbf{inv}(6 \mod 5, 5)}{5} \mod 6 \\ &\equiv \frac{1 - 6 * \mathbf{inv}(1, 5)}{5} \mod 6 \\ &\equiv \frac{1 - 6 * 1}{5} \mod 6 \\ &\equiv \frac{-5}{5} \mod 6 \\ &\equiv -1 \mod 6 \\ &\equiv 5 \mod 6. \end{aligned} \tag{55}$$

This recovers the result indicated previously, but with a more general computational approach that can be applied more broadly.

If $\text{GCD}(A, N) = 1$, then the congruence $Ax \equiv 1 \mod N$ is solved by

$$x \equiv \textbf{inv}(A, N) \mod N, \tag{56}$$

where

$$\textbf{inv}(A, N) = \begin{cases} 1 & \text{if } A \equiv 1 \mod N \\ \frac{1 - N * \textbf{inv}(N \mod A, A)}{A} \mod N & \text{if } A \not\equiv 1 \mod N \end{cases} \mod N. \tag{57}$$

This, combined with the previous commentary, will generally allow you to solve congruences $\mod N$, and in the same way as in the previous section, solve linear equations in integer variables.

GCD and Euclidean Algorithm

There remain two mathematical questions to process, or three depending on how motivated you are.

- How can you determine whether or not the GCD of A and N is 1?
- How can you be sure that this process for computing the inverse, repeatedly reducing the arguments via mods, will eventually terminate in the base case, i.e., $A = 1$?
- What is the big-O of this process?

As it turns out, all three of these questions can be addressed essentially at the same time, via **the Euclidean Algorithm**.

Given integers A, N, the greatest common divisor of A and N may be calculated via

$$\text{GCD}(A, N) = \begin{cases} N & \text{if } A = 0 \\ \text{GCD}(N \mod A, A) & \text{else.} \end{cases} \tag{58}$$

Note, this mimics the same 'argument reduction via mods' approach as taken in computing the inverse in the previous section - these two algorithms are really performing different versions of the same computation.

In the case of $\text{GCD}(5, 6)$, we get $\text{GCD}(5, 6) = \text{GCD}(1, 5) = \text{GCD}(0, 1) = 1$. For larger numbers, we have that $\text{GCD}(15, 21) = \text{GCD}(6, 15) = \text{GCD}(3, 6) = \text{GCD}(0, 3) = 3$. The algorithm essentially hinges on the idea that this process of repeatedly reducing via mods terminates at the GCD of the two numbers. In this way, we get immediately that the previous algorithm for computing inv will terminate with a base case of $A = 1$ in the case that the GCD is 1, because this process terminates at the GCD.

But why is this so? Consider expressing N as

$$N = A * k + (N \mod A), \tag{59}$$

for some integer k. In this case, we see that

$$N - A * k = (N \mod A), \tag{60}$$

in which case we get relatively immediately that any common factor of N and A must divide $N \mod A$ - in particular, the *greatest* common divisor of N and A must divide $(N \mod A)$, and further still

$$\text{GCD}(A, N) \text{ divides } (N \mod A) \text{ and } A \implies \text{GCD}(A, N) \text{ divides GCD}(N \mod A, A). \tag{61}$$

Similarly however, since

$$A * k + (N \mod A) = N, \tag{62}$$

we must get that any common divisor of A and $N \mod A$ must divide N - in particular, the *greatest* common divisor of A and $(N \mod A)$ must divide N. As above,

$$\text{GCD}(N \mod A, A) \text{ divides } N \text{ and } A \implies \text{GCD}(N \mod A, A) \text{ divides GCD}(A, N). \tag{63}$$

If X divides Y and Y divides X it must be (up to sign differences) that $X = Y$, i.e.,

$$\text{GCD}(N \mod A, A) \text{ divides GCD}(A, N). \tag{64}$$

The only exception to this is the base case when $A = 0$, since we cannot divide by 0 and hence $N \mod A$ will not exist.

This repeated mod process therefore must terminate (since the size of the arguments is being reduced each time) and must terminate in the GCD of both of the original numbers. If the GCD is 1, then the process for computing the inverse will terminate as desired.

This addresses the first two questions above. For the third, the big-O of this process, the overall computational complexity is governed by the length of this sequence of mods. Once the sequence is computed, computing the inverse is simply a matter of evaluating a constant number of operations for each mod in the sequence.

How long can this sequence run before terminating? This is actually an incredibly fast process, as the mod operation rapidly reduces the size of the relevant arguments. In fact, you can argue that $N \mod A \leq N/2$: if $A \geq N/2$, then $N \mod A = N - A \leq N/2$. If $A < N/2$, then enough A's can be 'packed' into N such that for some k, $N/2 \leq A * k \leq N$, which again (thinking of mods as remainders) will yield $N \mod A \leq N/2$. This implies that, tracking the arguments of the sequence of mods, we have

$$(A, N) \to (N \mod A, A) \to (A \mod N \mod A, N \mod A) \leq (A/2, N/2), \tag{65}$$

i.e., two steps of the mod sequence reduces both arguments by at least a factor of $1/2$. If A is the smaller of the two arguments, this implies that you are going to need, in the worst case, $\approx 2\log_2(A)$ many steps for the sequence to terminate, for an overall complexity of $O(\ln A)$. This is going to be an incredibly efficient algorithm.