Notes

September 5, 2014

7

$680 = 2^3 \cdot 5 \cdot 17, 2^3 \cdot 5 + 17 = 57, m, n = 40, 17$

8

$$\begin{aligned}(h, k) &= m \\ m|dh &\to m|a \\ m|dk &\to m|b\end{aligned}$$

12

$$\begin{aligned}(a, b) &= 1 \\ (a, c) &= 1 \\ &\Leftrightarrow \\ (a, [b, c]) &= 1\end{aligned}$$

19

p,q are twin primes, provethat pq+1 is square iff p,q are twin primes

$$\begin{aligned}q &= p + 2 \\ pq + 1 = p(p + 2) + 1 = p^2 + 2p + 1 &= (p + 1)^2 \\ m^2 &= pq + 1 \\ mm - 1 = pq(m + 1)(m - 1) &= pq \\ (a + 1) = pq, or 1 or p(a - 1) = 1, or pq, &or q\end{aligned}$$

23

$x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + ... + x + 1)$
$x^{2k+1} + 1 = (x + 1)(x^{2k} - x^{2k-1} + x^{2k-2} - ... + x^2 - x + 1)$

2^n+1 is prime is given. n is a power of two iff prime factorization of n is 2^m. prove by contradiction. assume there exists $p = 2k+1$ that divides n. $n = (2k+1)\cdot q$.

$$2^n + 1 = 2^{q(2k+1)}$$
$$= (2^q)^{2k+1} = (2^q+1)(2^{q2k} - 2^{q(2k-1)} + ... + 1)$$

now 2^n+1 is not prime unless $p = 1$ and p is prime

last time

$a, n \in \mathbb{Z}, n > 1$ the equation $ax \equiv 1 \mod n$ has a solution iff $(a, n) = 1$.

thm

$a, b, n \in \mathbb{Z}, n > 1$

1. the only eq $ax \equiv b \mod n$ has a solution iff $d|b$ where $d = \gcd(a, n)$.
2. assume that $d|b$ then the integer solutions of the equation are of the form $...x - \frac{2n}{d}, x - \frac{n}{d}, x, x + \frac{n}{d}, x + \frac{2n}{d}, ...$, in particular modulo n, there exist exactly d distinct solutions,namely $x, x + \frac{n}{d}, x + \frac{2n}{d}, ..., x + \frac{(d-1)n}{d}$

proof

assume that $ax \equiv b \mod n$ has a solutionn. then there exist $\alpha, q \in \mathbb{Z}$ such that $a\alpha - b = nq$. this implies that $b = a\alpha - nq \to d|b$ because $d|a\alpha$ and $d|nq$

assume $d|b$. then $b = d\beta$ for some $\beta \in \mathbb{Z}$

$$b = (as + nt)\beta, s, t \in \mathbb{Z}$$
$$as\beta \equiv b \mod n \to s\beta \text{ is a solution}$$

assume $d|b$, let $m = \frac{n}{d}$. claim α solution $\to \alpha + km$ solution for all $k \in \mathbb{Z}$.

proof of claim

α solution$\Rightarrow$ $a\alpha \equiv b \mod n$ but $a(\alpha + km) = a\alpha + akm$ and $akm = ak\frac{n}{d} = n\frac{a}{d}k \in \mathbb{Z}$ so $akm \equiv a\alpha \equiv b \mod n$

to finish we need to prove the following:

if α, β are solutions then $\beta - \alpha$ is a multiple of m.

$$a\alpha \equiv b \mod n$$
$$a\beta \equiv b \mod n$$
$$a\alpha \equiv a\beta \mod n$$
$$n|a(\beta - \alpha)$$
$$n = md$$
$$md|a(\beta - \alpha)$$
$$a = a'd$$
$$md|a'd(\beta - \alpha)$$
$$m|a'(\beta - \alpha)$$

if we know that gcd of m and a' is one then $m|(\beta - \alpha)$. we know it is because $md = n$ and $a = a'd$ and d is gcd of a, n so if there were another divisor then d wouldn't be the gcd, it would be pd.

chinese remainder theorem

$m, n \in \mathbb{Z}^+$ then the system $x \equiv a \mod n, x \equiv b \mod m$ has an integer solution iff m and n are relatively prime. moreover, any two solutions are congruent modulo mn.

proof

m,n are relatively prime, write $m\alpha + \beta n = 1$, let $x = a\alpha m + b\beta n$ then $x \equiv a\alpha m \equiv a \mod n$ because αm is congruent to 1. and $x \equiv b\beta n \equiv b \mod m$

exercises

second part of chinese remainder theorem