Appendix week 11

Contents

1 Unique factorization, gcd and lcm.

After the fundamental theorem of arithmetic we can write the decomposition of an integer into primes in two ways. Firstly

$$n = p_1 p_2 ... p_r$$

where the primes are not necessarily *distinct*. E.g. $20 = 2 \times 2 \times 5$. Alternatively

$$n = p_1^{a_1} p_2^{a_2} ... p_s^{a_s}$$

where the primes *are* distinct and the exponents $a_i \geq 0$ for all i. E.g. $20 = 2^2 \times 5$. It is important that we allow $a_i = 0$ (which you may feel is strange, since it says a prime is not in the decomposition and there are infinitely many primes not in the decomposition), but it is useful when considering two numbers simultaneously. E.g. if $a = 20$ and $b = 15$ then $a = 2^2 \times 3^0 \times 5^1$ while $15 = 2^0 \times 3^1 \times 5^1$.

In general, if a, b and c are integers > 1 let $p_1, p_2, ..., p_n$ be all the primes that divide abc. So we can write

$$a = \prod_{i=1}^{n} p_i^{a_i}, \quad b = \prod_{i=1}^{n} p_i^{b_i} \quad \text{and} \quad c = \prod_{i=1}^{n} p_i^{c_i},$$

for some exponents $a_i, b_i, c_i \geq 0$ for $1 \leq i \leq n$. Then $ab = c$ if,and only if, $a_i + b_i = c_i$ for all $1 \leq i \leq n$. This is because, by unique factorization, the number of times a prime divides ab equals the number of times it divides c. This leads to the following hopefully obvious conclusion,

$$\begin{aligned} a|c &\Leftrightarrow \exists b \geq 1 : ab = c \\ &\Leftrightarrow \exists b_i \geq 0 : a_i + b_i = c_i \quad \text{for all } 1 \leq i \leq n, \\ &\Leftrightarrow a_i \leq c_i \quad \text{for all } 1 \leq i \leq n. \end{aligned}$$

Theorem 1 *Let $p_1, p_2, ..., p_n$ be all the distinct primes that divide ab and write*

$$a = \prod_{i=1}^{n} p_i^{a_i} \quad \text{and} \quad b = \prod_{i=1}^{n} p_i^{b_i}$$

for some $a_i, b_i \geq 0$, $1 \leq i \leq n$. Then

$$\gcd(a, b) = \prod_{i=1}^{n} p_i^{\min(a_i, b_i)},$$

and

$$\text{lcm}(a, b) = \prod_{i=1}^{n} p_i^{\min(a_i, b_i)}.$$

Further

$$\gcd(a, b) \times \text{lcm}(a, b) = ab.$$

Proof If $d = \gcd(a, b)$ then $d|a$ and $d|b$. Thus the primes dividing d must divide both a and b, in particular they come from the list $p_1, p_2, ..., p_n$. Therefore

$$\gcd(a, b) = \prod_{i=1}^{n} p_i^{d_i}$$

for some $d_i \geq 0$ for $1 \leq i \leq n$. From above $d|a$ means that $d_i \leq a_i$ while $d|b$ means $d_i \leq b_i$. These combine as $d_i \leq \min(a_i, b_i)$, for all $1 \leq i \leq n$. But d is the *greatest* of all common divisors so we take equality, i.e. $d_i = \min(a_i, b_i)$.

For the lowest common multiple, recall the

Definition 2 *The* ***lowest common multiple*** *of integers a, b is the positive integer f that satisfies*

1) $a|f, b|f$,

2) if $a|k$, $b|k$ then $f|k$.

Note that ab is a multiple of both a and b and thus a common multiple. By part (2) of the definition $\text{lcm}(a,b)\,|ab$. In particular the primes dividing $\text{lcm}(a,b)$ come from the list $p_1, p_2, ..., p_n$. Therefore

$$\text{lcm}(a,b) = \prod_{i=1}^{n} p_i^{f_i}$$

for some $f_i \geq 0$ for $1 \leq i \leq n$.

The condition that $a|\,\text{lcm}(a,b)$ implies $a_i \leq f_i$ while $b|\,\text{lcm}(a,b)$ implies $b_i \leq f_i$ for $1 \leq i \leq n$. These combine to give $\max(a_i, b_i) \leq f_i$ for $1 \leq i \leq n$. But $\text{lcm}(a,b)$ is the *least* common multiple so we take $f_i = \max(a_i, b_i)$ for $1 \leq i \leq n$.

Finally, since for all x, y we have

$$\min(x,y) + \max(x,y) = x + y,$$

(student to check this), then

$$\begin{aligned}
\gcd(a,b) \times \text{lcm}(a,b) &= \prod_{i=1}^{n} p_i^{\min(a_i,b_i)} \prod_{i=1}^{n} p_i^{\max(a_i,b_i)} \\
&= \prod_{i=1}^{n} p_i^{\min(a_i,b_i)+\max(a_i,b_i)} \\
&= \prod_{i=1}^{n} p^{a_i+b_i} = \prod_{i=1}^{n} p^{a_i} \prod_{i=1}^{n} p^{b_i} \\
&= ab.
\end{aligned}$$

■

Example 3 *Find* $\gcd(235224, 63504)$ *and* $\text{lcm}(235224, 63504)$.

Solution.

$$a = 235224 = 2^3 3^5 11^2 \quad \text{and} \quad b = 63504 = 2^4 3^4 7^2.$$

Then

$$\begin{aligned}
\gcd(235224, 63504) &= 2^{\min(3,4)} 3^{\min(5,4)} 7^{\min(0,2)} 11^{\min(2,0)} \\
&= 2^3 3^4 7^0 11^0 \\
&= 648.
\end{aligned}$$

And

$$\begin{aligned}\operatorname{lcm}(235224, 63504) &= 2^{\max(3,4)}3^{\max(5,4)}7^{\max(0,2)}11^{\max(2,0)} \\ &= 2^4 3^5 7^2 11^2 \\ &= 23051952.\end{aligned}$$

Corollary 4

$$\gcd(a, b) = 1$$

if and only if none of the prime divisors of a divide b and vice-versa.

Aside You may feel inclined to use the prime factorization to find the greatest common divisors of two numbers instead of Euclid's algorithm. But since it is extremely hard to find the prime factors of very large numbers this method is of limited use.

2 Sieve of Eratosthenes

All the numbers from 2 up to 100

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Delete multiples of 2 apart from 2 itself:

	2	3	5	7	9
11		13	15	17	19
21		23	25	27	29
31		33	35	37	39
41		43	45	47	49
51		53	55	57	59
61		63	65	67	69
71		73	75	77	79
81		83	85	87	89
91		93	95	97	99

Delete multiples of 3 apart from 3 itself:

	2	3	5	7	
11		13		17	19
		23	25		29
31			35	37	
41		43		47	49
		53	55		59
61			65	67	
71		73		77	79
		83	85		89
91			95	97	

Delete multiples of 5 apart from 5 itself:

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	49
		53			59
61				67	
71		73		77	79
		83			89
91				97	

Delete multiples of 7 apart from 7 itself:

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	
		53			59
61				67	
71		73			79
		83			89
				97	

The next number is 11 which is greater than $\sqrt{100}$ and so there are no multiples of it less than 100 that haven't already been deleted in earlier stages. Thus we are left with the 25 primes <100.

3 Prime Numbers

For $x > 0$ let $\pi(x)$ be the number of primes not exceeding x. So $\pi(10) = 4$, $\pi(100) = 25$, (as seen from the application of the Sieve of Eratosthenes in the appendix), $\pi(1000) = 168$ and $\pi(5000) = 669$. Also

$$\pi\left(10^{23}\right) = 1,925,320,391,606,803,968,923,$$

due to Tomás Oliveira e Silva, 2007. Is there a simple formula for $\pi(x)$?

Theorem 5 *Prime Number Theorem (1896)*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1.$$

This means that we can make

$$\left| \frac{\pi(x)}{x/\ln x} - 1 \right|$$

as small as we like by taking x sufficiently large. This difference is < 0.054 if $x \geq 10^9$, is < 0.039 if $x \geq 10^{12}$ and is < 0.033 if $x \geq 10^{14}$. So, for very large x the graph for $\pi(x)$ lies close to that of $x/\ln x$.

Proof not given (until MATH31022 Analytic Number Theory).

On doing some calculations you might in fact think that $x/\ln x$ is not a very good approximation to $\pi(x)$. If $f(x) = x/\ln x$ then

$$f\left(10^{23}\right) = 1,888,236,877,840,225,337,613.6039952...$$

which seems quite a long way short of the true value of $\pi(10^{23})$ above.

(See http://en.wikipedia.org/wiki/Prime-counting_function for further details including a description of a better approximation to $\pi(x)$.)

4 Example of use of unique factorization

Example 6 *For all integers $m \geq 2$ there is **no** rational solution to $q^m = 2$.*

Solution by contradiction. Assume that for some $m \geq 2$ there exists a rational $q : q^m = 2$.

Write $q = a/b$ with $a, b \in \mathbb{Z}$, so we get $a^m = 2b^m$.

Firstly, $|b| \geq 1$ and so $|a^m| = 2|b|^m \geq 2$. Thus $|a| \geq 2$. Substitute back in to get $2|b|^m = |a|^m \geq 2^m$, that is, $|b|^m \geq 2^{m-1} \geq 2$ since $m \geq 2$. Therefore we have both $|a| > 1$ and $|b| > 1$. This means that both a and b can be factored into primes.

Let $p_1, ..., p_n$ be the primes dividing either a or b. We can then write

$$a = \prod_{i=1}^{n} p_i^{a_i} \text{ and } b = \prod_{i=1}^{n} p_i^{b_i}$$

for exponents $a_i \geq 0$ and $b_i \geq 0$. Substitute into $a^m = 2b^m$ to get

$$\prod_{i=1}^{n} p_i^{ma_i} = 2 \prod_{i=1}^{n} p_i^{mb_i}.$$

Since 2 appears in the factorisation on the Right Hand Side we have, by unique factorisation that 2 must appear in the product on the Left Hand Side. Without loss of generalisation assume $p_1 = 2$ in which case $a_1 \geq 1$. We then get

$$2^{ma_1} \prod_{i=2}^{n} p_i^{ma_i} = 2^{1+mb_1} \prod_{i=2}^{n} p_i^{mb_i}.$$

By unique factorization the number of 2's on both sides are identical so $ma_1 = 1 + mb_1$, i.e. $m(a_1 - b_1) = 1$ in which case m divides 1. This contradicts $m \geq 2$ and so the assumption is false and thus for no $m \geq 2$ can we find a rational solution of $q^m = 2$. ■

One of the first proofs you examine at University is to prove that $\sqrt{2}$ is irrational, i.e. no *rational* solutions of $q^2 = 2$. So here we have extended this result.

5 What are $\phi(100)$ and $\phi(1000)$?

Lemma 7 *For* $m \geq 2$

$$\phi(10^m) = 10\phi\left(10^{m-1}\right).$$

Proof Note first that by looking at the prime divisors of n and a we have $\gcd(n, a^m) = 1 \Leftrightarrow \gcd(n, a) = 1$. With $a = 10$ we deduce that

$$\phi(10^m) = |\{1 \leq n \leq 10^m, \gcd(n, 10) = 1\}|. \quad (1)$$

Simply write every $1 \leq n \leq 10^m$ as $r + s10^{m-1}$ with $1 \leq r \leq 10^{m-1}$ and $0 \leq s \leq 9$. Then

$$\begin{aligned} \gcd(n, 10) = 1 &\Leftrightarrow \gcd\left(r + s10^{m-1}, 10\right) = 1 \\ &\Leftrightarrow \gcd(r, 10) = 1. \end{aligned}$$

Hence

$$\begin{aligned} \phi(10^m) &= \left|\left\{0 \leq r \leq 10^{m-1}, 0 \leq s \leq 9 : \gcd(r, 10) = 1\right\}\right| \\ &= 10 \times \left|\left\{0 \leq r \leq 10^{m-1} : \gcd(r, 10) = 1\right\}\right| \\ &\qquad \text{since there are 10 choices for } s, \\ &= 10 \times \phi\left(10^{m-1}\right), \end{aligned}$$

by (1) with m replaced by $m-1$. ■

Repeated use of the Lemma gives

$$\phi\left(10^m\right) = 10^{m-1}\phi\left(10\right) = 4 \times 10^{m-1}.$$

So $\phi\left(100\right) = 40$ and $\phi\left(1000\right) = 400$.

Example 8 *Find the last three digits of* 13^{1010}.

Solution We need calculate $13^{1010} \bmod 1000$. From above $\phi\left(1000\right) = 10\phi\left(100\right) = 400$, and so $13^{400} \equiv 1 \bmod 1000$. Thus

$$13^{1010} \equiv \left(13^{400}\right)^2 13^{210} \equiv 13^{210} \bmod 1000.$$

Repeated squaring gives

$$\begin{aligned}
13^2 &= 169, \\
13^4 &\equiv 169^2 = 28561 \equiv 561 \bmod 1000, \\
13^8 &\equiv 561^2 = 314721 \equiv 721 \bmod 1000, \\
13^{16} &\equiv 721^2 = 519841 \equiv 841 \bmod 1000, \\
13^{32} &\equiv 841^2 = 707281 \equiv 281 \bmod 1000, \\
13^{64} &\equiv 281^2 = 78961 \equiv 961 \bmod 1000, \\
13^{128} &\equiv 961^2 = 923521 \equiv 521 \bmod 1000.
\end{aligned}$$

Combine

$$\begin{aligned}
13^{210} &= 13^{128} \times 13^{64} \times 13^{16} \times 13^2 \\
&\equiv 521 \times 961 \times 841 \times 169 \\
&= 500681 \times 142129 \\
&\equiv 681 \times 129 \\
&= 87849 \\
&\equiv 849 \bmod 1000.
\end{aligned}$$

Hence the last 3 digits of 13^{1010} are 849. ■

6 If $\gcd(r, n) = 1$ and $\gcd(a, n) = 1$ then $\gcd(ar, n) = 1$.

The following result was used implicitly in a proof in the lectures, perhaps you didn't notice. If so, look back to see where it was used. The proof of the lemma can be based on the fact that the gcd is 1 if the integers have no prime divisors in common. Here we will base the proof on the earlier result that the gcd is 1 if there exists a linear combination of the integers which equals 1.

Lemma 9 *If* $\gcd(r, n) = 1$ *and* $\gcd(a, n) = 1$ *then* $\gcd(ar, n) = 1$.

Proof An earlier result on coprime integers stated that if $\gcd(r, n) = 1$ and $\gcd(a, n) = 1$ then $\exists k, \ell, s, t \in \mathbb{Z}$, for which

$$kr + \ell n = 1 \quad \text{and} \quad sa + tn = 1.$$

Rearrange as $kr = 1 - \ell n$, $sa = 1 - tn$, multiply together and rearrange as

$$(ks)\, ra + (\ell + t - \ell t n)\, n = 1.$$

Since we have a linear combination of ra and n equaling 1 we deduce that $\gcd(ra, n) = 1$. ■

7 $\phi(mn) = \phi(m)\,\phi(n)$

We now give a rather long proof concerning the Euler phi function on products. A shorter proof will be given in MATH31022.

Theorem 10 *If* $\gcd(m, n) = 1$ *then* $\phi(mn) = \phi(m)\,\phi(n)$.

Proof Let

$$R = \{r_1, r_2, ..., r_{\phi(m)}\} = \{1 \le r \le m : \gcd(r, m) = 1\}$$

and

$$S = \{s_1, s_2, ..., s_{\phi(n)}\} = \{1 \le s \le n : \gcd(s, n) = 1\},$$

be the reduced residue systems for the respective moduli m and n.

We are to show that the set of $\phi(m)\phi(n)$ integers:

$$T = \{nr + ms : r \in R, s \in S\}$$

is a reduced residue system for modulus mn.

Note that T can be written as an array

$$\begin{array}{llllll}
nr_1 + ms_1 & nr_1 + ms_2 & nr_1 + ms_2 & \cdots & \cdots & nr_1 + ms_{\phi(n)} \\
nr_2 + ms_1 & nr_2 + ms_2 & & & & \vdots \\
nr_3 + ms_1 & & & & & \vdots \\
\vdots & & & & & \vdots \\
\vdots & & & & & \vdots \\
nr_{\phi(m)} + ms_1 & \cdots & \cdots & \cdots & \cdots & nr_{\phi(m)} + ms_{\phi(n)}
\end{array}$$

and we see $\phi(m)\,\phi(n)$ terms in this array.

We will establish the following:

- Each integer in T is co-prime to mn;
- No two integers in T are congruent modulo mn;
- Each integer co-prime to mn is congruent modulo mn to one of these integers in T.

We prove each in turn:

1. Assume for contradiction that there exists an element of T **not** co-prime to mn, so there exist $r \in R, s \in S$ such that $\gcd(nr + ms, mn) > 1$.

   Suppose p is a prime divisor of this $\gcd(nr + ms, mn)$. Then $p|(nr + ms)$ and $p|mn$.

   As p divides mn but $\gcd(m, n) = 1$ then p either divides m or n *but not both*.

   Suppose WLOG that $p|m$.

   Then $p|m$ and $p|(nr + ms)$ which together imply $p|nr$. But p either divides m or n *but not both* so $p|m$ means $p \nmid n$. Combining $p|nr$ and $p \nmid n$ gives us $p|r$.

   But now we have both $p|m$ and $p|r$, and so $p|\gcd(r, m)$, which contradicts $\gcd(r, m) = 1$.

   Similarly if $p|n$ we get a contradiction with $\gcd(s, n) = 1$.

   So there is **no** prime divisor of $\gcd(nr + ms, mn)$ and hence $\gcd(nr + ms, mn) = 1$. Thus all elements of T are co-prime to mn.

2. Assume for contradiction that two integers in T **are** congruent modulo mn.

   Thus there exist $(r, s), (r', s') \in R\times S$, with $nr+ms \equiv nr'+ms' (\operatorname{mod} mn)$ and $(r, s) \neq (r', s')$.

   The congruence $nr + ms \equiv nr' + ms' (\operatorname{mod} mn)$ rearranges as

   $$n(r - r') + m(s - s') = kmn$$

   for some $k \in \mathbb{Z}$. As m divides two of these terms it must divide the third, so $m|n(r - r')$.

   By the assumption in the Theorem, $\gcd(m, n) = 1$ which with $m|n(r - r')$ implies $m|(r - r')$, or $r \equiv r' (\operatorname{mod} m)$.

   Yet r and r' are part of the same reduced residue system modulo m, so $r = r'$.

   Similarly, from looking at n we get $s = s'$.

   Thus $(r, s) = (r', s')$, contradicting the $(r, s) \neq (r', s')$ above.

   Hence distinct elements of T cannot be congruent modulo mn.

3. Let $k \in \mathbb{Z} : \gcd(k, mn) = 1$. We wish to show that k is congruent to some element of T modulo mn.

   Since $\gcd(m, n) = 1$ and $1|k$ we can use Euclid's Algorithm say, to write $k = nr' + ms'$ for some $r', s' \in \mathbb{Z}$.

   Suppose that r' is **not** coprime to m, i.e. $\gcd(r', m) > 1$. There would then exist some prime number p such that $p|m$ and $p|r'$.

   Such a prime would be a common divisor of both $k = nr' + ms'$ and mn, contradicting $\gcd(k, mn) = 1$.

   Hence $\gcd(r', m) = 1$ and so r' is congruent modulo m to one of the integers in R.

   By the same argument, $\gcd(s', n) = 1$ and so s' is congruent modulo n to one of the integers in S.

   Writing $r' = r + am$, $s' = s + bn$ with $r \in R, s \in S$ we have

   $$k = nr' + ms' = nr + ms + mn(a + b) \equiv nr + ms \operatorname{mod} mn$$

   and $nr + ms \in T$.

Further examples of the use of Euler's and Fermat's Theorems.

Example 11 *Show that* $2^{1194}+1$ *is divisible by 65.*

Solution We need show that $65|\left(2^{1194}+1\right)$. Since $65=5\times 13$ we need show that $5|\left(2^{1194}+1\right)$ and $13|\left(2^{1194}+1\right)$.

First, 5 is prime so by Fermat's Little Theorem we have $2^4\equiv 1 \bmod 5$. Hence

$$\begin{aligned}2^{1194}+1 &= \left(2^4\right)^{298}2^2+1\equiv 1^{298}\times 4+1\\ &= 5\equiv 0 \bmod 5.\end{aligned}$$

Next, 13 is prime so again by Fermat's Little Theorem we have $2^{12}\equiv 1 \bmod 13$. Hence

$$\begin{aligned}2^{1194}+1 &= \left(2^{12}\right)^{99}2^6+1\equiv 1^{99}\times 64+1\\ &= 65\equiv 0 \bmod 13.\end{aligned}$$

Combining these we get the required result. ■

Example 12 *Is 221 prime?*

Solution Fermat's Little Theorem tells us that *If* 221 is prime *then* $2^{220}\equiv 1 \bmod 221$. Note that

$$\begin{aligned}220 &= 128+64+16+8+4\\ &= 2^7+2^6+2^4+2^3+2^2.\end{aligned}$$

Look at powers of 2 modulo 221.

n	$2^{2^n}=\left(2^{2^{n-1}}\right)^2 \bmod 221$
0	2
1	$2^2=4$
2	$4^2=16$
3	$16^2=256\equiv 35$
4	$35^2=1225\equiv 120\equiv -101$
5	$(-101)^2=10201\equiv 35$
6	$35^2\equiv -101$
7	$(-101)^2\equiv 35.$

So

$$\begin{aligned} 2^{220} &= 2^{2^7}2^{2^6}2^{2^4}2^{2^3}2^{2^2} \\ &\equiv 35 \times (-101) \times (-101) \times 35 \times 16 \\ &\equiv 220 \times 220 \times 16 \\ &\equiv 16 \bmod 221. \end{aligned}$$

Since $2^{220} \not\equiv 1 \bmod 221$ we deduce that 221 is **not** prime. ■

Example 13 *You now notice that 221 is composite and in fact* $221 = 17 \times 13$. *Use Fermat's Little Theorem, **and not the method of successive squaring** modulo 221, to check that* $2^{220} \equiv 16 \bmod 221$.

Solution. If $x \equiv 2^{220} \bmod (17 \times 13)$ then

$$x \equiv 2^{220} \bmod 17 \quad \text{and} \quad x \equiv 2^{220} \bmod 13.$$

By Fermat's Little Theorem we have $2^{16} \equiv 1 \bmod 17$ so

$$\begin{aligned} 2^{220} &= 2^{13\times16+12} \equiv 2^{12} \equiv \left(2^4\right)^3 \\ &\equiv (-1)^3 \equiv -1 \equiv 16 \bmod 17. \end{aligned}$$

Similarly $2^{12} \equiv 1 \bmod 13$ so

$$2^{220} = 2^{18\times12+4} \equiv 2^4 = 16 \equiv 3 \bmod 13.$$

Thus our two equations become

$$x \equiv 16 \bmod 17 \quad \text{and} \quad x \equiv 3 \bmod 13$$

Such a system was solved in the Appendix to Chapter 3, using the Chinese Remainder Theorem, where we found $x \equiv 16 \bmod 221$. ■

Example 14 *Solve* $x^{22} + x^{11} \equiv 2 \bmod 11$.

Solution Any solution must have $\gcd(x, 11) = 1$ and so, by By Fermat's Little Theorem, $x^{10} \equiv 1 \bmod 11$. Thus

$$\begin{aligned} x^{22} + x^{11} &\equiv x^2 + x \\ &\equiv x^2 + 12x \quad \text{on adding 11 to make the coefficient even,} \\ &\equiv (x+6)^2 - 36 \bmod 11, \end{aligned}$$

by completing the square. Thus we need only solve $(x+6)^2 - 36 \equiv 2 \bmod 11$, i.e. $(x+6)^2 \equiv 5 \bmod 11$. From the table

y	$y^2 \bmod 11$
1	1
2	4
3	9
4	5
5	3

we see that $y^2 \equiv 5 \bmod 11$ iff $y \equiv 4$ or $-4 \bmod 11$. Thus we get two solutions to our congruence of $x + 6 \equiv 4 \bmod 11$ and $x + 6 \equiv -4 \bmod 11$, i.e. $x \equiv 1$ or $9 \bmod 11$. ■

Example 15 *Show that there are no integer solutions* (x, y) *to*

$$x^{12} - 11x^6y^5 + y^{10} \equiv 8.$$

Solution We assume for a contradiction that there *are* integer solutions. When we look at this modulo 11 they will remain solutions.

There are three cases.

Firstly, it maybe that $11|y$ in which case the equation becomes $x^{12} \equiv 8 \bmod 11$. For any solution of this we must have $\gcd(x, 11) = 1$ so, again by Fermat's Theorem, $x^{10} \equiv 1 \bmod 11$ and so we get $x^2 \equiv 8 \bmod 11$. From the table above we see this has no solutions.

Secondly, $11 \nmid y$ and $11|x$ when the equation becomes $y^{10} \equiv 8 \bmod 11$. But Fermat's Little Theorem gives $y^{10} \equiv 1 \bmod 11$. Thus there are no solutions.

Finally, $11 \nmid y$ and $11 \nmid x$. So Fermat's Theorem again gives both $x^{10}, y^{10} \equiv 1 \bmod 11$. Thus

$$x^{12} - 11x^6y^5 + y^{10} \equiv x^2 + 1 \bmod 11,$$

and so we are looking for solutions to $x^2 \equiv 7 \bmod 11$. Again from the table we see this has no solution.

In all cases our equation has *no* solutions modulo 11. This contradiction means our original equation has no integer solutions. ■

In the MATH10101 2008 exam we find

Example 16 *Show that there are no integer solutions* (x, y) *to*

$$7x^2 - 35xy + 5y^{14} = 88.$$

Solution Left to student but, for a hint, look at this modulo 7.

2 Wilson's Theorem.

Recall that

$$\begin{aligned}\mathbb{Z}_m^* &= \{[r]_m : 1 \le r \le m, \gcd(r,m) = 1\} \\ &= \{[r]_m : 1 \le r \le m, \exists\, [x]_m \in \mathbb{Z}_m : [r]_m [x]_m = [1]_m\}.\end{aligned}$$

Question What $1 \le r \le m$ are self-inverse modulo m, i.e. for which we can we take $[x]_m = [r]_m$ in $[r]_m [x]_m = [1]_m$? In other words, for which $1 \le r \le m$ do we have $r^2 \equiv 1 \bmod m$?

Answer given here only for $m = p$, prime.

Theorem 17 *$x^2 \equiv 1 \bmod p$ if, and only if, $x \equiv 1$ or $-1 \bmod p$.*

Proof

$$\begin{aligned}x^2 \equiv 1 \bmod p &\Leftrightarrow p | \left(x^2 - 1\right) \\ &\Leftrightarrow p | (x-1)(x+1) \\ &\Leftrightarrow p | (x-1) \text{ or } p | (x+1) \quad \text{since } p \text{ prime} \\ &\Leftrightarrow x \equiv 1 \bmod p \quad \text{or} \quad x \equiv -1 \bmod p.\end{aligned}$$

■

Thus the only self-inverses in $\mathbb{Z}_p^*$ are $[1]_p$ and $[p-1]_p$. As a corollary of this we have

Theorem 18 *Wilson's Theorem. If p is prime then*

$$(p-1)! \equiv -1 \bmod p.$$

Proof p.291. Take the product of all the classes in $\mathbb{Z}_p^*$:

$$\prod_{\substack{1 \le r \le p-1 \\ \gcd(r,p)=1}} [r]_p \,.$$

Rearrange, pairing up a class with its inverse, leaving $[1]_p$ and $[p-1]_p$ unpaired. So the product becomes

$$[1]_p \left(\prod_{\text{pairs}} [r]_p [r]_p^{-1} \right) [p-1]_p = [p-1]_p \,.$$

Thus
$$\prod_{\substack{1\le r\le p-1\\ \gcd(r,p)=1}} [r]_p = [p-1]_p\,,$$
which is equivalent to the stated result. ■

Example 19 *Calculate* $20! \bmod 23$.

Solution 23 is a prime so Wilson's Theorem gives $22! \equiv -1 \bmod 23$. But
$$\begin{aligned} 22! &= 22\times 21\times 20! \equiv (-1)\times(-2)\times 20! \\ &\equiv 2\times 20! \bmod 23. \end{aligned}$$

By observation 12 is the inverse of 2 modulo 23 so
$$\begin{aligned} 20! &\equiv (12\times 2)\times 20! = 12\times(2\times 20!) \\ &\equiv 12\times 22! \text{from above}, \\ &\equiv -12 \text{ from } 22! \equiv -1 \bmod 23, \\ &\equiv 11 \bmod 12. \end{aligned}$$