7.2 Applications of Euler's and Fermat's Theorem.

i) Solving non-linear congruences.

Example Find a solution to $x^{12} \equiv 3 \bmod 11$.

Solution Any solution of this must satisfy $\gcd(x, 11) = 1$ so Fermat's Little Theorem gives $x^{10} \equiv 1 \bmod 11$. Thus our equation becomes

$$3 \equiv x^{12} \equiv x^2 x^{10} \equiv x^2 \bmod 11.$$

Now check.

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

Note that if $x \geq 6$ then $11 - x \leq 5$ and $x^2 \equiv (11 - x)^2 \bmod 11$ so all possible values of $x^2 \bmod 11$ will be seen in the table.

From the table we see **an** answer is $x \equiv 5 \bmod 11$. ■

ii) Example Show that $x^5 \equiv 3 \bmod 11$ has **no** solutions.

Solution by contradiction. Assume $x^5 \equiv 3 \bmod 11$ has solutions. Any solution of this must satisfy $\gcd(x, 11) = 1$ so Fermat's Little Theorem gives $x^{10} \equiv 1 \bmod 11$. Since $5|10$ we square both sides of the congruence to get

$$1 \equiv x^{10} \equiv \left(x^5\right)^2 \equiv 3^2 \equiv 9 \bmod 11.$$

This is false and so the assumption is false and thus the congruence has no solution. ■

iii) Example Find *a* solution to $x^7 \equiv 3 \bmod 11$.

Solution Again $x^{10} \equiv 1 \bmod 11$ by Fermat's Little Theorem but this time $7 \nmid 10$, in fact $\gcd(7, 10) = 1$. From Euclid's Algorithm we get

$$3 \times 7 - 2 \times 10 = 1. \qquad (1)$$

Raise both sides of the congruence to the third power to get

$$\begin{aligned} 3^3 &\equiv \left(x^7\right)^3 \equiv x^{3\times 7} \equiv x^{1+2\times 10} \text{ by } (1), \\ &\equiv x\left(x^{10}\right)^2 \\ &\equiv x \bmod 11. \end{aligned}$$

Hence **a** solution is $x \equiv 3^3 \equiv 5 \bmod 11$.

Don't forget to check your answer (by successive squaring of 5). ■

iv) **Example** Find the last two digits of 13^{1010}, (asked for in Chapter 3).

$$13^{1010} = \left(13^{40}\right)^{25} 13^{10} \equiv 1^{25} 13^{10} \equiv 13^{10} \bmod 100.$$

Hence, using (**??**) ,

$$\begin{aligned} 13^{1010} &\equiv 13^{10} = 13^8 \times 13^2 \\ 21 \times 69 &\equiv 49 \bmod 100. \end{aligned}$$

Therefore, the last two digits of 13^{1010} are 49.

Question for students. What are the last *three* digits of 13^{1010}? See appendix.

v) Is $2^{35}+1$ divisible by 11? Here we look at $2^{35}+1 \bmod 11$. Because 11 is prime we could use Fermat's Little Theorem to say $2^{10} \equiv 1 \bmod 11$. Thus

$$2^{35}+1 \equiv 2^5+1 \equiv 32+1 = 33 \equiv 0 \bmod 11,$$

i.e. $2^{35}+1$ is divisible by 11. ■

Question for students. Show that $2^{1194}+1$ is divisible by 65.

Appendix

Contents

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

Example 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 $13|\left(2^{1194}+1\right)$.

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

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

13 is prime so again by Fermat's Little Theorem we have $2^{12} \equiv 1 \bmod 5$. 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 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 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

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

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

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

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 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

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

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

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

we see that two solutions are $x+6 \equiv 4 \bmod 11$ and $x+6 \equiv -4 \bmod 11$, i.e. $x \equiv 1$ or $9 \bmod 11$. ■

Example 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.

First, 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. ■

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

Proof

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

■

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

Theorem *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 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

$$\begin{aligned} 20! &\equiv (12 \times 2) \times 20! = 12 \times (2 \times 20!) \\ &\equiv 12 \times 22! \text{ from above,} \\ &\equiv -12 \text{ from } 22! \equiv -1 \bmod 23, \\ &\equiv 11 \bmod 12. \end{aligned}$$