Problem for 2005 April

Communicated by Dan Jurca

Prove that for each positive integer m there exists an integer solution x of the following congruence.

$$(x^2-5)(x^2-401)(x^2-2005) \equiv 0 \pmod{m}$$

Solution by Gagan Sekhon and an anonymous solver, edited by Dan Jurca

We prove the somewhat more general result: if u and v are distinct odd primes, and $v \equiv 1 \pmod 8$, and v is a quadratic residue (mod u), then for each positive integer m there exists an integer x such that $(x^2-u)(x^2-v)(x^2-uv) \equiv 0 \pmod m$. (By the law of quadratic reciprocity it follows that also u is a quadratic residue (mod v).) This will certainly prove the assertion above, since 5 and 401 are distinct odd primes, $401=50\times8+1$, $2005=5\times401$, and $1^2 \equiv 401 \pmod 5$. (Also $178^2 \equiv 5 \pmod{401}$.)

Reference: Ivan Niven and H.S.Zuckerman, *An Introduction to the Theory of Numbers*, 4th edition, sections 2.3, 2.5, 2.6, and 3.2.

Our proof consists of the following steps.

1. We show that for each positive integer r there exists a positive integer x such that $(x^2-u)(x^2-v)(x^2-uv) \equiv 0 \pmod{2^r}$.
2. We show that for each odd prime p there exists a positive integer x such that $(x^2-u)(x^2-v)(x^2-uv) \equiv 0 \pmod p$.
3. We show that for each odd prime p and each positive integer r there exists a positive integer x such that $(x^2-u)(x^2-v)(x^2-uv) \equiv 0 \pmod{p^r}$.
4. Finally, by the Chinese remainder theorem it will follow that for each positive integer m there exists a positive integer x such that $(x^2-u)(x^2-v)(x^2-uv) \equiv 0 \pmod m$.

1. We shall use the following lemma and its corollary.
   Lemma. Suppose that e is an even integer, and r is a nonnegative integer; then there exists a nonnegative integer i such that $2^r \mid (i^2+i-e)$.

Proof.
We shall use induction on r, the assertion being clear if r=0 or if r=1, since then $2^r|(0^2+0-e)$, as e is even. Now suppose $2 \le r$ and $2^{r-1}|(j^2+j-e)$, say $(j^2+j-e)=2^{r-1}\cdot n$. Then let

$$i=\begin{cases} j+2^r & \text{if n is even,} \\ j+2^{r-1} & \text{if n is odd.} \end{cases}$$

Then if n is even, say n=2m, we find

$$\begin{aligned} i^2+i-e &= (j+2^r)^2+(j+2^r)-e \\ &= (j^2+j-e)+2^r(2j+2^r+1) \\ &= 2^{r-1}\cdot n+2^r(2j+2^r+1) \\ &= 2^{r-1}\cdot 2m+2^r(2j+2^r+1) \\ &= 2^r(m+2j+2^r+1); \end{aligned}$$

and if n is odd, say n=2m+1, we find

$$\begin{aligned} i^2+i-e &= (j+2^{r-1})^2+(j+2^{r-1})-e \\ &= (j^2+j-e)+2^{r-1}(2j+2^{r-1}+1) \\ &= 2^{r-1}\cdot n+2^{r-1}(2j+2^{r-1}+1) \\ &= 2^{r-1}(2m+1+2j+2^{r-1}+1) \\ &= 2^r(m+j+2^{r-2}+1); \end{aligned}$$

so that in either case $2^r|(i^2+i-e)$. Thus the lemma follows by induction on r.

Corollary. If $q \equiv 1 \pmod 8$, and r is a nonnegative integer, then there exists an integer x such that $x^2-q \equiv 0 \pmod{2^r}$.
Proof.
If r=0, then any integer x will do; if r=1, then any odd x will do. Suppose $2 \le r$. Then if q=8s+1, there exists an integer i such that $2^{r-2}|(i^2+i-2s)$. With x=2i+1 we have $x^2-q=4i^2+4i+1-8s-1=4(i^2+i-2s)$, which is clearly divisible by 2^r, so that $x^2-q \equiv 0 \pmod{2^r}$.
Since by hypothesis $v \equiv 1 \pmod 8$, this completes step 1.

2.

The assertion in step 2 follows at once if p=u or p=v, so suppose $p \ne u$ and $p \ne v$.

Recall the Legendre symbol where p is an odd prime and a is relatively prime to p:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if a is a quadratic residue mod p,} \\ -1 & \text{if a is not a quadratic residue mod p,} \end{cases}$$

and the relation

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Each of these equals 1 or −1, so with a=u and b=v at least one of them equals 1, completing step 2.

3.

We shall use this lemma, proved using the method in section 2.6 of the text cited above.
Lemma. Suppose p is an odd prime, p does not divide w, and $a^2-w \equiv 0 \pmod p$. Then for each positive integer r there exists an integer x such that $x^2-w \equiv 0 \pmod{p^r}$.
Proof.
We shall use induction on r, the case r=1 being given in the hypothesis. Suppose $2 \le r$ and $b^2-w \equiv 0 \pmod{p^{r-1}}$, say $b^2-w=q\cdot p^{r-1}$. Since p does not divide w, it follows that p does not divide b; and of course p does not divide 2. Therefore, since $\mathbf{Z}_p$ is a field, there exists an integer c such that $2b\cdot c \equiv 1 \pmod p$, say $2b\cdot c=d\cdot p+1$. Then with $t=-q\cdot c$ we have

$$\begin{aligned} (b+tp^{r-1})^2-w &= b^2+2btp^{r-1}+t^2p^{2r-2}-w \\ &= (b^2-w)+2btp^{r-1}+(t^2p^{r-2})p^r \\ &= qp^{r-1}+2btp^{r-1}+(t^2p^{r-2})p^r \\ &= (q+2b\cdot t)p^{r-1}+(t^2p^{r-2})p^r \\ &= (q+2b\cdot -qc)p^{r-1}+(t^2p^{r-2})p^r \\ &= q(1-2bc)p^{r-1}+(t^2p^{r-2})p^r \\ &= q(1-dp-1)p^{r-1}+(t^2p^{r-2})p^r \\ &= (-dq+t^2p^{r-2})p^r, \end{aligned}$$

whence with $x=b+tp^{r-1}$ we have $x^2-w \equiv 0 \pmod{p^r}$, and the lemma follows from induction on r.
Now if p=u we can use this lemma and the fact that v is a quadratic residue (mod u) to deduce that for each positive integer r there exists an integer x such that $x^2-v \equiv 0 \pmod{p^r}$; and similarly in the case p=v. In case $p \ne u$ and $p \ne v$ we use the fact that at

least one of u, v, uv is a quadratic residue (mod p), proved in step 2, and hence for each positive integer r there exists x such that $(x^2-u)(x^2-v)(x^2-uv) \equiv 0 \pmod{p^r}$. This completes step 3.

4.

Now suppose the positive integer $m=p_1^{e_1}\times p_2^{e_2}\times\ldots\times p_k^{e_k}$ where the p_i are distinct primes and the e_i are positive integers. By steps 1 and 3 for each i, $1 \le i \le k$, there exists x_i such that
$(x_i^2-u)(x_i^2-v)(x_i^2-uv) \equiv 0 \pmod{p_i^{e_i}}$. By the Chinese remainder theorem there exists an integer x such that

$$\begin{aligned} x &\equiv x_1 \pmod{p_1^{e_1}} \quad \text{and} \\ x &\equiv x_2 \pmod{p_2^{e_2}} \quad \text{and} \\ &\vdots \\ x &\equiv x_k \pmod{p_k^{e_k}}; \end{aligned}$$

clearly for this x we have

$$(x^2-u)(x^2-v)(x^2-uv) \equiv 0 \pmod{m},$$

as desired.