F10

• KTR 2

Rep. $\equiv \pmod n$; respects $+, -, \cdot$. Exponents ?

Thm (Fermat) p prime $\Rightarrow$ $a^{p-1} \equiv 1 \pmod p$ if $p \nmid a$ (V1)

$a^p \equiv a \pmod p$ $\forall a$ (V2)

Ex. Reduce $6^{322} \pmod{17}$

Pf of Fermat.

at least mention [Primality testing (ave-dir; cf $4^{14} \equiv 1 \pmod{15}$), Carmichael numbers: $561 = 3 \cdot 11 \cdot 17$]

• Cryptography: Alice, Bob, Eve. $f_{enc}^{-1} = f_{dec}$.

• Caesar, symm. cipher ⇝ practical problems

• Asymmetric cipher; public/private key

• RSA • Keys: (n,e), d (ABT: (n,k), a)

• encryption, decryption

Ex. a) Show: $(n,e) = (33,7)$, $d = 3$ is a valid RSA key pair.

b) Encrypt "2".

c) Decrypt result.

should have time [• Proof that $(m^e)^d \equiv m$ $\forall m$.]

Ex. Bob's public key is $(85,13)$. Eve intercepts ciphertext "6".

Plaintext ?

if time [Discuss security, "recent issues" signatures ?]